

Managing the risks of inconsistent internet connectivity to businesses across sub-Saharan Africa

Gavin Moss

Student Number: 1543307

A research article submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Business Administration

Johannesburg, 2018

Protocol number: WBS/BA1543307/310

DECLARATION

I, Gavin Moss, declare that this research article is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration in the Graduate School of Business Administration, University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

A handwritten signature in black ink, appearing to be 'Gavin Moss', written on a light blue background.

Gavin Moss

Signed at Sandton, on the 28th day of February 2018

DEDICATION

This research report is dedicated to my two favourite people, my wife, Bryony and my daughter, Juniper. However, Juniper is too young to read and Bryony does not find this subject very enthralling, so they will probably never know that they are the reason for all this work, to make their lives better.

ACKNOWLEDGEMENTS

I would like to acknowledge my supervisor, Antony Soicher, who understood that these had been the longest two years of my life, and helped me get this assignment completed with as many helpful hints as possible.

I would also like to thank all my close friends, including H. Simpson, N. Flanders, J. Lebowski, J. Bond, J. Bourne, S. Holmes, L. Croft and C. Brown who have not seen very much of me over the past two years; this has probably improved their lives not having to put up with my whisky infused drivel as often as before.

Thank you to the following people for proofreading, editing and improving my ineloquent use of the English language in many instances throughout this report: Darryl Moss, Ana Ferreira, Kate Wayman, Jenny Croll, Andrew and Malcolm Drummond.

Lastly, I would like to thank my fellow students who have gone through the last two years of this together with me, and have provided hours of fun, support and shoulders to cry on as we have all immersed ourselves in this process together.

SUPPLEMENTARY INFORMATION

Nominated journal:

The African Journal of
Information Systems

Supervisor / Co-author:

Antony Soicher

Word count: 13,779

ABSTRACT

The global economy is becoming more congruent as technology advances at an exponential pace, and communities are taking on new digital dimensions wherever one looks. In sub-Saharan Africa specifically, there is an opportunity for digitisation to create new, transformative tools that ultimately increase the competitiveness of Africa's economies on a global scale. However, the public needs to trust that their access to the internet will not be disrupted, otherwise the increase in utilisation and development of the digital economy across the continent will continue to lag behind more developed economies.

While risk management has always been a core requirement for organisations, leaders are increasingly aware of the need to manage new digital risks, for example, cyber security, driven by rapidly changing technology and continually advancing global internet connectivity. Faced with ever-changing and potentially catastrophic cyber threats, organisations must start treating digital risk management as a truly strategic concern, not confined to an isolated silo of risk analysts.

The purpose of this research is to investigate whether the inherent risks of inconsistent internet connectivity across sub-Saharan Africa are adequately managed, and if not, how best to improve the current approach.

The data collection procedure included conducting interviews across different communities within the sample population to include people who have a background in risk analysis, people who have experienced internet connectivity failures that impact their purchasing habits online and service providers who can measure internet outages.

Based on the content of the interviews conducted by the author, the conclusion is that the risks of inconsistent internet connectivity across sub-Saharan Africa are not adequately managed. Current risk management frameworks are not holistic in their approach to risks, potentially impacting e-commerce and the digital economy.

INTRODUCTION

Purpose of the study

The ever-improving digital economy is fast becoming an enabler to countries' economies across sub-Saharan Africa. If internet connectivity can become more consistent for businesses and consumers, this in turn, has the potential to improve countries' economies, GDP's and the quality of life for many of sub-Saharan Africa's population. Internet availability has also offered many Africans an opportunity to achieve key development aims, improve education levels, health services, insurance, and employment opportunities.

The purpose of this research was to investigate whether the inherent risks of inconsistent internet connectivity across sub-Saharan Africa are adequately managed. By quantifying the major risk factors and applying them to industry standard risk models, this study attempted to make recommendations on how best to mitigate these risks, and if necessary, discuss proposed changes to standard risk management practices.

Context of the study

This research report focuses on commercial industries utilising digital customer channels based within sub-Saharan Africa. It is not industry specific, but rather spans the digital economy and reviews how inconsistent internet connectivity affects profitability, and how this is managed from a risk perspective.

The uptake of digital channels offered within multiple sectors places ever more reliance on the quality of this service which is underpinned by technology, and the risk of this technology not being available, which should be carefully quantified and managed. Many companies rely on a digital channel as the single-entry point for new and recurring customers to purchase goods or services. Without internet connectivity, these businesses have no other way of reaching their customers.

The study is based on business results over the past two years, as a longer timespan would potentially be skewed by the dramatic decrease in the cost of

internet connectivity within the same period. However, this is dependent on the country and its unique regulations governing telecommunications.

	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017
Egypt	3.1	2.8	2.8	1.7	1.4	1.2
Tanzania	6.0	0.9	2.4	3.0	2.3	2.3
Ghana	3.9	3.9	2.5	2.5	2.3	2.3
Nigeria	5.1	4.9	3.2	3.2	3.2	3.1

Figure 1 - 1GB Mobile Data Costs in USD (Research ICT Africa, 2017)

The researcher's intention was to overlay the utilisation of internet based customer channels and network connectivity to understand what the customer experiences were like, how this affects organisations' profitability, and any risk mitigation strategies to help improve availability of these digital channels.

Problem Statement

This study investigates how the risks of inconsistent internet connectivity to the digital economy across sub-Saharan Africa are quantified and managed.

Significance of the study

The study provides guidance to businesses operating within sub-Saharan Africa on how to quantify and mitigate risks of inconsistent internet connectivity on the digital economy. If this risk mitigation is performed correctly, it could have a direct positive impact on the profitability of the organisation, help to increase transaction numbers via digital channels and allow a more consistent customer experience.

Delimitations of the study

- This study includes interview responses from within the financial, risk and telecoms industries across sub-Saharan Africa.

- This study does not include any organisations that do not maintain a sub-Saharan African footprint.
- This study is limited to reported instances of network connectivity downtime across the mainstream media, and data obtained from multiple organisations with operations across sub-Saharan Africa.

Definition of terms

- ADSL – Asymmetric Digital Subscriber Line. Data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide
- COSO – Committee of Sponsoring Organizations of the Treadway Commission. This is a joint initiative to combat corporate fraud and dedicated to guide executive management and governance entities on relevant aspects of organizational governance.
- DRC – Democratic Republic of Congo. A country in central western Africa
- EABS – East African Backhaul System. A terrestrial fibre optic cable network linking East African countries to the submarine fibre-optic cables along the East African coast
- EASSy – Eastern Africa Submarine Cable System. An undersea fibre optic cable system connecting countries in East Africa to the rest of the world
- GDP – Gross Domestic Product. A monetary measure of the market value of all the final goods and services produced in a period for a country
- POS – Point of Sale. Where a customer tenders' payment in exchange for goods or services
- SAT-3 – South Atlantic 3. An undersea fibre optic cable system linking Portugal and Spain to South Africa, with connections to several West African countries along the route
- TEAMS – The East African Marine System. An undersea fibre optic cable system connecting countries in East Africa to the rest of the world
- WACS – West Africa Cable System. An undersea fibre optic cable system connecting countries in West Africa to the rest of the world

Assumptions

- Most sub-Saharan African countries have similar constraints around the availability of high speed terrestrial ADSL (asymmetric digital subscriber line) connectivity, and much of the population utilises mobile data as their main means of connection to the internet.
- Most respondents completing the survey reflect normal perspectives based on their own experience
- Organisations and individuals across sub-Saharan Africa are aware of the economic opportunities presented by the digital economy.

LITERATURE REVIEW

Introduction

The global economy is becoming more congruent as technology advances at an exponential pace, and communities are taking on new digital dimensions wherever one looks. According to (Siemens, 2017), Africa is on a similar trajectory to developed economies and there is an opportunity for digitisation to create new, transformative tools that ultimately should increase the competitiveness of Africa's economies on a global scale.

Digital technology is vital for the economic development of countries' economies, and Africa has enjoyed exponential growth towards providing affordable internet access for all (World Bank Group, 2016). However, government-directed internet outages have become more commonplace across the continent in recent years (West, 2016), which can negatively affect a country's GDP (Gross Domestic Product) (Katz, 2012), (Belson, 2017) rather than simply attempting to control the flow of information.

The rise of the digital economy across sub-Saharan Africa brings with it many changes, for example, the ease and safety of purchasing every day household items via mobile money solutions. These changes to peoples' lives also include new risk elements that people and organisations need to be cognisant of, for example, cybersecurity risks, and the risk of the digital channel not being available because of inconsistent internet connectivity.

Growth of Africa's Digital Economy

Africa's Connection to the Rest of the World

Prior to 2009, only one older-generation undersea cable (SAT-3) connected the west of Africa to Europe, and most African countries relied on relatively expensive satellite connections for internet connectivity (Dhliwayo, 2005), (Peroni & Bartolo, 2018). On average, access to the internet, prior to 2009, cost Africans 50-100

times more than consumers in Europe, Asia and North America (Twinomugisha, 2010), (Kshetri, Rural e-Commerce in Developing Countries, 2018). Between 2009 and 2012, seven underwater fibre-optic cables were connected along the east and west coasts of the continent (Forden, The Undersea Cable Boom in Sub-Saharan Africa, 2015). Over the longer term, this infrastructure is set to benefit the public by contributing to the further reduction in data costs when connecting to the internet. The principal recipients to date have been multinational companies functioning in Africa (Forden, The Undersea Cable Boom in Sub-Saharan Africa, 2015).

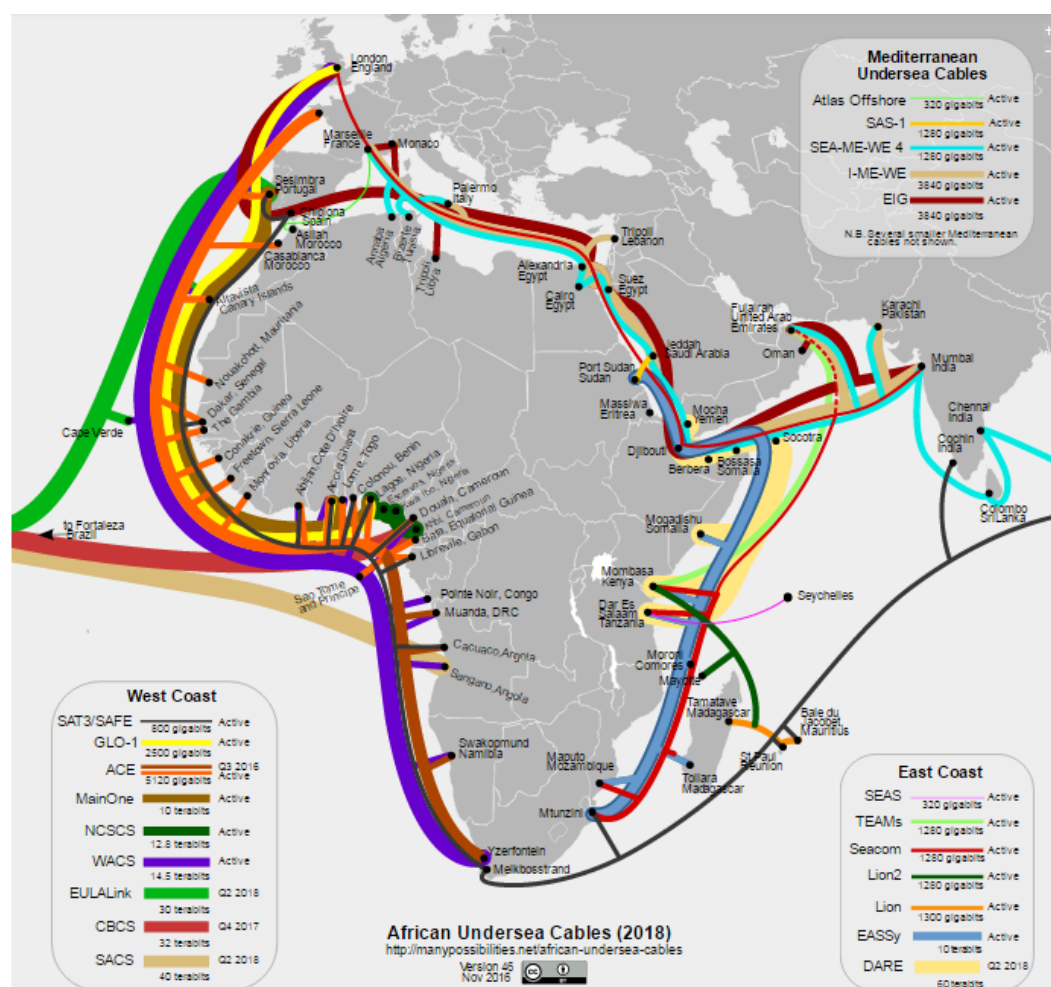


Figure 2 - African Undersea Cable Network (Many Possibilities, 2016)

Africa's Internet Connectivity Growth

Africa has made substantial advances in internet connectivity in the past ten years. Internet penetration has grown by more than 400 per cent, while

international bandwidth has increased by over 2000 per cent between 2009 and 2014, mainly driven by the delivery of these undersea fibre-optic cables (Nyirenda-Jere & Biru, 2015), (Oyelaran-Oyeyinka & Adeya, 2004). Although the internet penetration volumes have increased exponentially, many African countries still have less than 10 per cent internet penetration, which correlates to an additional 1.38 per cent in annual GDP growth within low and middle-income economies (Katz, 2012), (Belson, 2017). These growth levels are often less than the inflation levels of the respective countries, so in effect, this is a nett contraction of the economies.

(World Bank Group, 2016) describes how the delivery of multiple undersea cables along the African coastlines has significantly reduced data costs, however, relatively high prices persist, compared to those of developed countries. Many landlocked African countries have difficulty in accessing these fibre-optic backbones and pay on average \$232 more per household per month for broadband access than those living in coastal areas (Dahir, Internet shutdowns continue to cost Africa's economies, 2017). This is unaffordable in relation to the average annual individual income of \$762 per household in many areas of sub-Saharan Africa (Lakner & Milanovic, 2013), (Chinn & Fairlie, 2010)

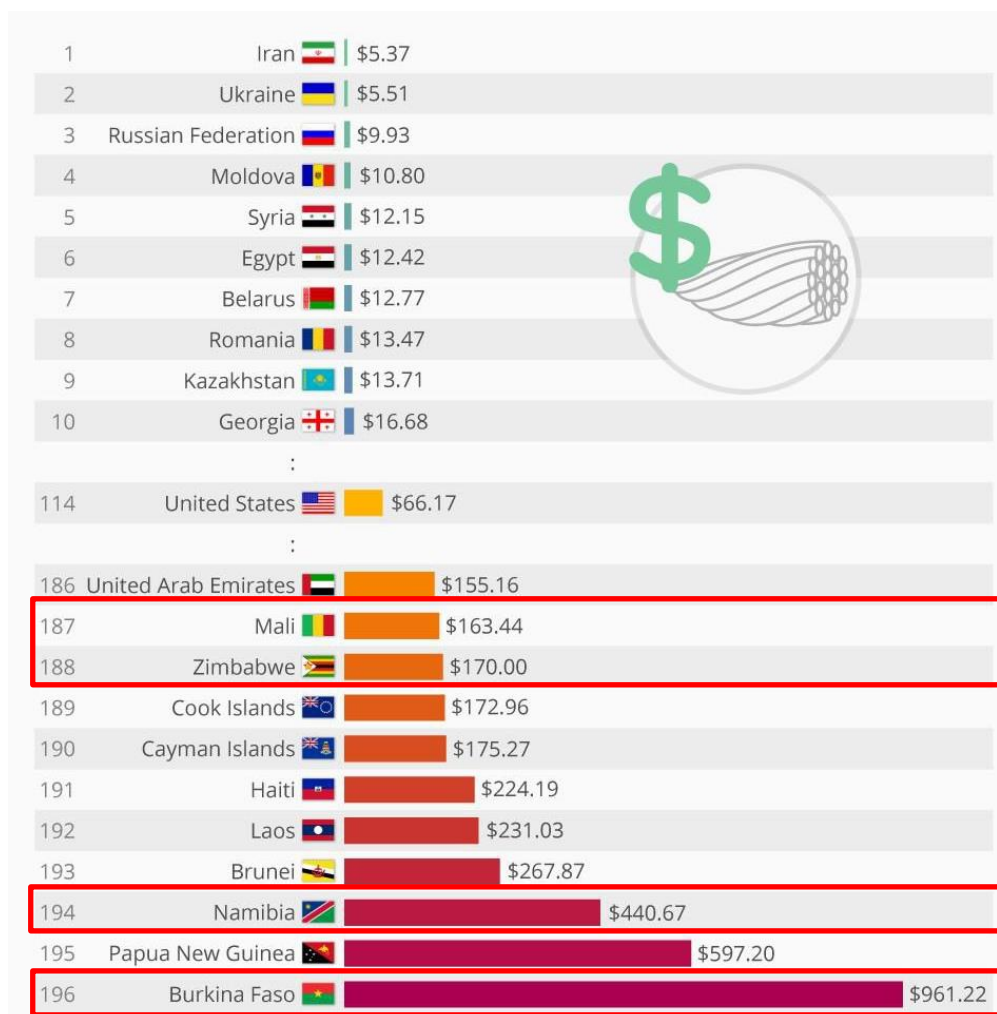


Figure 3 - Internet Access Costs Per Month (USD) (McCarthy, 2017)

Smartphones and mobile data, on the other hand, have significantly dropped in price over the past five years, with the number of smartphone connections across the continent increasing by nearly 100 per cent (Stork, Calandro, & Gillwald, 2013). Mobile phone sales prices have dropped from an average of \$230 in 2012 to between \$50 and \$100 in 2017 (Matinde, 2017), and the average monthly use of mobile data has increased from 0.3GB to 4.3GB per capita over the past five years (The GSM Association, 2016).

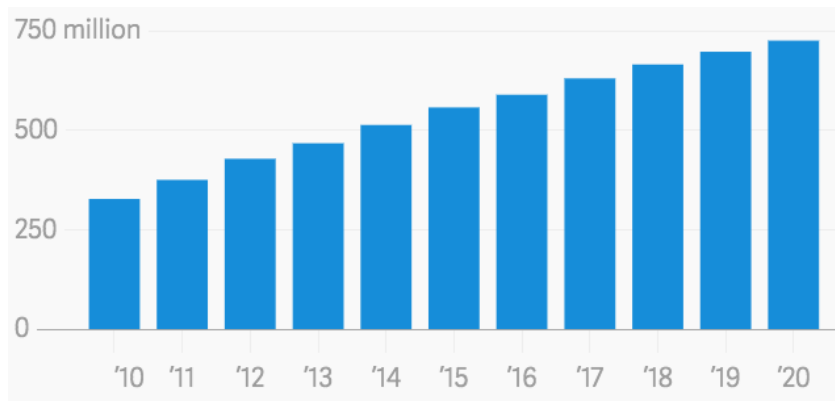


Figure 4 - Unique Mobile Subscribers in Africa (The GSM Association, 2016)

Africa's Digital Economy

The digital economy incorporates financial events directly related to internet use, encompassing infrastructure investment, internet accessibility, use and access, which ultimately leads to online consumer expenditure (Goldstuck, 2012). Internet access in Africa is still relatively expensive compared to developed countries, and this confines consumers' internet access and utilisation, leading to lower than expected internet traffic volumes and related revenues (Mbarika, Jensen, & Meso, 2002). However, Africa's middle class is on the increase, with approximately 30 per cent of the continent falling within this bracket and is expected to grow to 42 per cent by 2060 (Ncube, Lufumpa, & Kayizzi-Mugerwa, 2011), which will equate to more than one billion people.

Africa's digital economy annual growth rate is approximately 25.8 per cent which far outperforms the global rate of 16.8 per cent (Busha, 2014). However, despite vast potential, the African digital economy still has challenges to overcome (Kshetri, Barriers to e-commerce and competitive business models in developing countries: A case study, 2007) Research shows a 90 per cent correlation between technology investment and socio-economic development across sub-Saharan Africa, and connectivity and digital services will play a major role in driving sustainable inclusive growth (Madkour, 2018). Ekekwe (2015), and du Plessis & Boon (2004) point out that many large e-commerce ventures across the continent continue to struggle, which indicates that Africa's digital economy is in the process of maturing. Even Jumia, part of AIG (African Internet Group), which is

defined as Africa's first unicorn (a company valued at over \$1 billion), has yet to turn a profit (Hsu, 2016).

The main factor hampering the growth of the digital economy is the inconsistent internet connectivity across the continent (Roycroft & Anantho, 2003), (Kende, 2017). Meanwhile, in South Africa, Kenya and Nigeria, the bulk of internet users now shop online (Wynne, Berthon, Pitt, Ewing, & Napoli, 2001), (Nkemdilim, 2015), and with deepening internet penetration across Africa (growth of over 8000 per cent from 2000 to 2017), increasing numbers of consumer transactions are being completed online. Internet Usage Statistics (2017) predict that 50 per cent of the continent will have internet access by 2025 and, based on online shopping patterns in other parts of the world, e-commerce in Africa could account for up to 10 per cent of retail sales, or \$75 billion (Internet Usage Statistics, 2017).



Figure 5 - Top 3 African e-commerce Economies (Mohammed, 2015)

Intermittent Internet Connectivity Across Africa

Until recently, the SEACOM cable was the only fibre-optic based backbone that supplied a large portion of the data connectivity to sub-Saharan Africa, and although this solution has provided better speeds and connectivity in general, there are often faults with the undersea cables that cause an intermittent loss of connection to multiple countries. In recent years, the SEACOM service was unavailable in March 2015 and January and October 2016 (van Zyl, 2016), because of damage to the undersea cable. Because of the instability of the

services providing internet connectivity, as well as large areas to cover, the internet penetration across Africa is lower than everywhere else in the world.

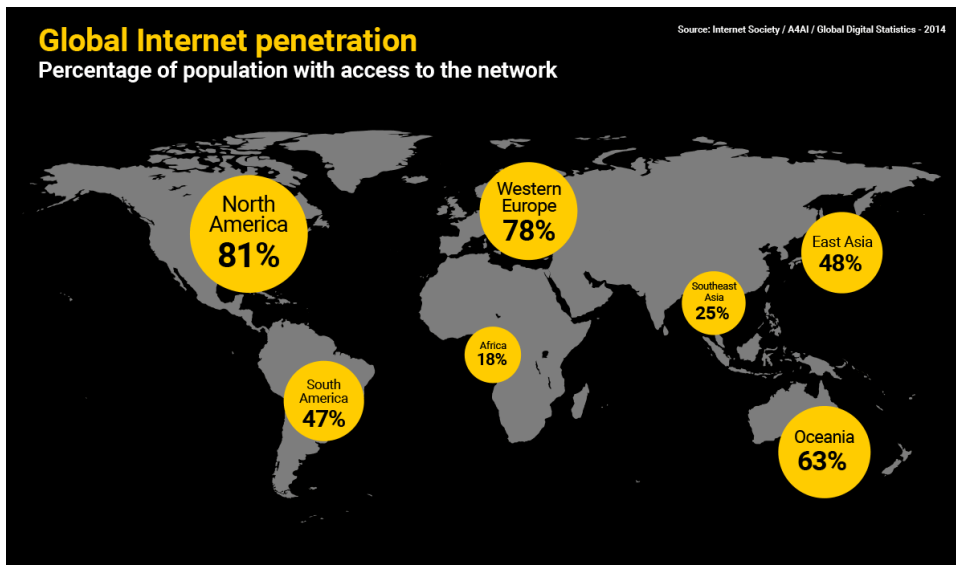


Figure 6 - Global Internet Penetration (Swart, 2014)

In 2016, there were at least 56 shutdowns of the internet around the world, most of them across the African continent (Zittrain, et al., 2017). These shutdowns affect individuals and organisations that depend on the internet, and the reasons for the shut-downs vary from infrastructure outages to government-controlled shutdowns in an attempt to limit the flow of information (Bekele, 2017).

In 2016, across Africa alone, 11 countries governments disrupted internet communications, often during elections. The internet outages also can inflict serious damage to the economies of these countries that desperately seek growth (West, 2016). Muhumuza (2017) discusses how an internet shutdown perpetrated by the government in Uganda in February 2016 during the recent elections, correlated to over \$8 million lost from the country's GDP in just five days of internet restrictions.

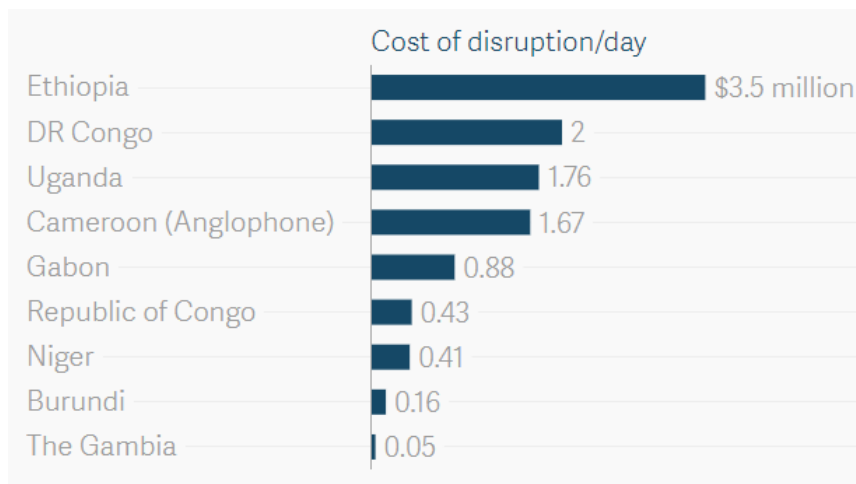


Figure 7 - Country Costs of Internet Disruption Per Day (Dahir, Internet shutdowns continue to cost Africa's economies, 2017)

Risk Management Practices are not Aligned to the sub-Saharan African Digital Economy

Current Risk Management Frameworks

1. The Sarbanes-Oxley Act of 2002 aims to protect investors from the possibility of fraudulent accounting activities by organisations. Improvements in financial disclosures and electronic records management are two of the key areas that focus on risk management of an organisation on behalf of its investors (Senate and House of Representatives of the United States of America, 2002).
2. The German corporate governance code details legislative principles and standards by which German listed companies should be managed that promote responsible corporate governance (Deutscher Corporate Governance Kodex, 2017). Within this standard is the directive that the management board ensures appropriate risk management across the organisation.

3. The enterprise risk management integrated framework was published in 2004, and has gained broad acceptance by organisations in their efforts to manage risk (Committee of Sponsoring Organisations, 2004).
4. The King IV report on corporate governance is not a true risk management framework because its aim is primarily good corporate governance. However, it is important to mention because it reinforces the notion that good corporate governance is a holistic and interrelated set of arrangements to be understood and implemented in an integrated manner. The aim of the principles is to ensure that good governance is not just a tick-box exercise, but rather a lever for value creation (PwC, 2016).

Risk management frameworks are generally aligned to the ISO 31000 standard, which provides a set of principles, a framework and a procedure for the management of risk (Lark, 2015). ISO 31010 is a supportive standard for ISO 31000 that provides guidance on the collection and application of systematic methods for risk assessment (International Organization for Standardization, 2009). However, this standard does not provide guidance on how to identify risks or detailed instructions on how to manage risk.

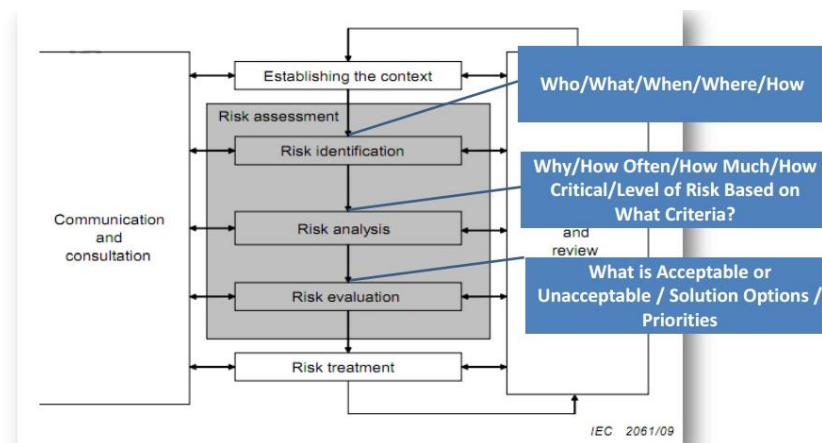


Figure 8 - ISO 31010 Risk Assessment Techniques (International Organization for Standardization, 2009)

Digital Risk Management in Africa

Corporate governance in Africa is not as highly regulated as in Europe, and practices relating to corporate risk management are not as advanced. van Wyk (2015) highlights that Africa has a lower percentage of early stage-risk mitigation in organisations (16 per cent) compared to global counterparts (35 per cent). While risk-taking is an essential practice in business, the cost of failures is frequently miscalculated (González, 2005). Corporate governance should thus ensure that risks are understood and managed effectively to maximise business value (OECD, 2014).

(Passenheim, 2010) and (Rasmussen, 1997) discuss how many organisations still look at risks in isolation and unless they are identified, analysed and controlled together, the risk dependencies may remain unnoticed. Boehm (1989) shows that risk management is primarily focused on avoiding repetition of errors, and does not consider the constantly changing environment. New digital channels are unlocking opportunities and increasing challenges for organisations, including quick response times and constant digital channel availability. In a constantly connected world, consumers expect constant availability of digital channels (Pirner & Eschner, 2017). These include the likes of mobile banking channels, and ride-sharing applications, like Uber.

(Liew, Bellens, & Webster, 2016) detail how the management of digital risk is becoming more important because threats such as technology outages causing data loss and cybercrime are impacting business profitability on an increasing scale. The current risk policies and frameworks might not be adequate to address these fresh and growing digital risks (Stoneburner, Goguen, & Feringa, 2002), (Wolke, 2017). Traditional risk management practices are aligned to operational units within a business, and the management of the risk can become siloed. While this level of specialisation is essential to manage specific risk factors appropriately, compartmentalising risk managers can stifle the organisations best, holistic approaches to risk management (Layton, 2007), (Wolke, 2017).

E-commerce channels are subjected to technical risk factors to which other channels are not. Digital risks are not limited to one silo of business operations,

and cannot be managed in isolation. Storm (2017) discusses when business is conducted over the internet, technical issues with the infrastructure or networks can cause system unavailability, while malevolent hackers can expose sensitive customer data (Song, Fink, & Jeschke, 2018). Seck, Belai, & Nwuke (2014) argue that cybercrime is an increasing threat worldwide and is growing at a more rapid rate across Africa than in any other region of the world (Symantec Corporation, 2013). Cybersecurity specialists estimate that more than 80 per cent of computers across Africa are infected with malicious software (Gady, 2010), (My Broadband, 2018).

According to (Trevor, Inglis, & Heard, 2016), internet connectivity is governed by five key points: price of data, available bandwidth, technology security, connection latency and real estate for data centres. Internet connectivity infrastructure spans from the internal networks of the organisation to all third parties involved in the channel offering, ending with the client's data provider. When any of these points fail, the user will not be able to initiate a digital transaction, and this could lead to reputational, operational, systemic and liquidity risk for the organisation (Denyes & Lonie, 2016).

(Folpmers, 2016) discusses the concept of how current risk classification systems are outdated, and new approaches should be investigated to cater for the reliance on digitisation of all parts within organisations. The current risk taxonomy does not address new risks, for example, what if blockchain technology completely replaces current payment systems, but people still do not have access to online methods of payment to utilise this technology?

Proposition

To manage the risks of inconsistent internet connectivity to businesses across sub-Saharan Africa more effectively, there are three approaches that a combination of the research and available literature tend towards:

1. These risks can be adequately managed by enhancing current risk frameworks to include a digital sub-section within each risk category.

2. Current risk management frameworks do not cater for emerging digital risks like inconsistent internet connectivity, especially as the frameworks are outdated and do not change as quickly as technology, therefore new methods of managing these risks are required.
3. Current risk management frameworks should be combined with predictive analytics to broaden the approach to managing risk by providing a more holistic approach to risk management.

Conclusion of Literature Review

Economically, e-commerce already contributes \$18 billion or 1.1 per cent to the GDP of the continent, which is comparatively small equated to global averages of four per cent. The growth of the internet has been driven by many undersea cables along the east and west coasts of the continent which have enabled progressively faster access, declining costs of internet capable devices and the exponential growth of technology and users.

However, to date, internet users across the African continent are not yet benefiting from the cost reductions that were expected relatively quickly from this proliferation of intercontinental bandwidth. Limited internet access is not only due to high data costs and lack of internet penetration, but also because of African governments intent on limiting information flow during vital times.

Organisations that rely on the internet as a digital customer channel should be aware that current risk management practices are not aligned to the African digital economy (Folpmers, 2016), and in order to ensure continued business growth the inherent risks of the digital economy across Africa should be quantified and managed more effectively (Kossovsky, 2014).

RESEARCH METHODOLOGY

To achieve the general and specific objectives stated in the introduction, the author employed qualitative methods. The qualitative methods were as follows:

1. Interviews to gauge the relevant subject's opinion and outlook in a detailed and inclusive manner.
2. Action research that involved collaborative analysis to identify and analyse the underlying causes of the issues by active investigation.

Research methodology / paradigm

(Denzin & Lincoln, 2005) describe the process of qualitative research as an interpretive realistic slant to the world, which describes the study of situations within natural surroundings, and how people interpret these. The qualitative research utilised in this study involved semi-structured interviews, observation, and content analysis. Because of this, the information gathered could be subjective based on the individual's opinion and perspective of the issue under discussion, which (Rossman & Rallis, 2012) define as interpretivism.

This research assignment focuses on the constructivist / interpretivist paradigm as they are directly related concepts that address understanding the world as others experience it. This approach relies on the fact that knowledge is subjective and socially constructed, therefore interviewing the correct samples within the right population should allow candidates to answer based on relevant personal experiences.

The constructivist paradigm is a naturalistic inquiry method in which the researcher does not attempt to manipulate the phenomenon of interest. Therefore, the reliability of the results is dependent on the level of subjectivity the researcher applies during the results analysis. By ensuring that the study demonstrates what exists and is accurate, the validity of the research instrument should help ensure the reliability of the results.

Research Design

The qualitative approach to this research assignment targeted industry experts via interviews and action research across various pan-African organisations that rely on clients accessing their digital channels via the internet across sub-Saharan Africa.

This research sought to understand how the risks of internet outages on the digital economy in sub-Saharan Africa are managed and mitigated using standard risk modelling techniques. The research strategy attempted to ensure that the study answered the appropriate research questions and/or objectives in an economical, valid and reliable manner (Cooper & Schindler, 2006).

Population and sample

Population

The population includes everyone involved in businesses with digital channels, or who utilise the internet to access these channels, and who live in sub-Saharan Africa. The population also requires access to the internet which helps provide or utilise these digital channels.

Sample and sampling method

The author selected respondents to interview based on access and availability for face-to-face interviews, and made use of in-depth semi-structured interviews and written documents to collect and analyse the data. To collect the data, the target sample included a relevant subset of the population in the study, and purposive sampling was conducted, based on pre-selected criteria focused on the research question.

The research instrument

This study utilised semi-structured interviews as the main vehicle for data gathering, as this is the ideal way for contributors to discuss their views and give

their opinion of the matter in question (Kvale, 1996). Cohen, Manion, & Morrison (2000) argue that the process of an interview is not simply concerned with the data collection of the respondent's life experiences, but rather part of life itself.

Procedure for data collection

The data collection procedure included conducting semi-structured interviews across different communities within the sample to include people who have a background in risk analysis, people who have experienced internet connectivity failures that impact either their online purchasing habits or service providers whose digital channels have been affected by inconsistent internet connectivity.

Data analysis and interpretation

Once the interviews were completed, the records of the discussions were reviewed by the author, and by arranging, re-framing or otherwise exploring the data, the author identified patterns and insights applicable to the key research issue. The transcripts of these interviews are available upon request.

Limitations of the study

- The sample group is small in comparison to the number of businesses that provide digital based channels over the internet for customers across sub-Saharan Africa.
- A certain degree of subjectivity can be found across the interviews, based on recent events that may have directly impacted the respondents, for example, a recent internet outage affecting the respondent

PRESENTATION OF RESULTS

Introduction

This research elicited the opinions and perceptions of how adequately current risk management guidelines covered specific digital risks, like inconsistent network connectivity, that have arisen out of the digital economy within sub-Saharan Africa. The research was based on a series of semi-structured interviews with a range of participants including risk management practitioners, client relationship managers, business unit heads and technology unit heads.

In this chapter, the responses of the candidates to the semi-structured questions asked in the interviews are summarised. The author collated the responses into themes that emerged post the interviews. In the final section of this chapter, the author summarised the outcomes from these interviews.

Results

Management of technology risks in the digital economy across sub-Saharan Africa

The digital economy has transformed faster than the way organisations manage risks, and the continued pace of technological change is at odds with the traditional risk frameworks that have remained relatively static. Because of this rate of change, there is often a misalignment with risk management practitioners and technical teams, making risk management a very difficult task. Risk management involves detailed analysis of potential threats, and there are currently no real-time methodologies that can be applied rapidly enough to match the rate of changing digital risks. Therefore, risk management currently relies on historical data, rather than real-time information for threat identification.

Regional Risk Approaches

Risks will differ in countries and regions across sub-Saharan Africa. As an example: Kenya compared to the DRC (Democratic Republic of the Congo),

where Kenya has a highly digitised economy and as a result, a higher exposure to the inherent risks of doing business in that kind of economy. The DRC, on the other hand, has very low internet penetration and therefore low levels of digitisation. The main indicative factors causing the low penetration in the DRC include the vast expanse of the country as well as the continued political turmoil.

An initial evaluation of a country's digital capabilities could help inform the basic risk profile in each country. From this consolidated view of these countries, it is then possible to evaluate larger regions, such as west, east, south and central Africa. This consolidation of historical risks can be very helpful for new entities to quickly quantify initial risks. However, current risk frameworks do not always provide tangible examples of risks in each risk category, and this could lead to imminent threats being ignored because emerging organisations do not have a frame of reference of historical risks. As an example, larger organisations that operate across countries within sub-Saharan Africa may already understand the political risks inherent in a country based on their knowledge of the surrounding areas, however new entrants to that market may not.

Risk management maturity also differs across countries, for example, Nigeria and South Africa are leaders in risk management analytics across sub-Saharan Africa, whereas countries like Uganda still have some way to go. Digital risk management is a relatively new field across sub-Saharan Africa. There are not enough skills to effectively mitigate risks and provide forward-looking strategies, unless an organisation utilises external risk managers, or has a presence in other countries that have better risk managers who can be utilised.

Technology Improvements

In the digital economy, there is a heavy reliance on technology to derive income rather than an holistic view of the organisation's strategy and goals which, in turn, inform the technology strategy and direction. It stands to reason that technical teams manage technology, and therefore are best informed as to the potential technological and digital risks. In addition, many non-technical users do not truly understand the inherent risks within the digital economy, and how this relates to their business aspirations.

The profile of digital risk has increased significantly over the past few years, which, in turn, has brought a better level of maturity and investment into telecommunications and data centre infrastructure. As mentioned in chapter two, prior to 2009, only one undersea cable connected the west of Africa to Europe. Since then, sub-Saharan Africa has moved from a single internet backbone to multiple service providers, and the service, as well as the management of the inherent risks, has improved significantly. However, the number of undersea cables terminated along the African coastline has not generated the exponential growth of last-mile providers expected by the technology industry, and in turn, further reducing the costs of internet connectivity.

The additional investment in infrastructure goes together with improving the client experience, because the number of challenges related to networks is reducing. However, the risks of change-related outages have increased because of the increasing level of technology changes and the focus for technology and risk teams should now turn towards the internal technology stack to resolve issues, rather than on improvements to the internet backbone.

Practical Approaches to Risk Management

Many organisations seem comfortable managing risks on a theoretical basis, however risk management should be able to change as risks and technologies change. Risks cannot be isolated across the digital economy when they potentially impact the entire value chain of an organisation. As an example, cybercrime could well affect all aspects of an organisation from financial to reputational issues and is not limited to a silo of an organisation.

Currently, risk management is a separate function from technical delivery, and although potential risks are mitigated against standard frameworks, the number of online failures persist. This is more prevalent across sub-Saharan Africa, where the underlying network infrastructure is not stable enough to provide a consistent service to organisations. Risk management is therefore not consistently applied across technology. For example, payment systems that are accessed from within an organisation may require additional physical security around access to terminals to ensure the risk of fraud is reduced as much as

possible. However, physical access management measures such as these are not always effective enough, and because these risks are not managed consistently, the clients are not receiving a consistent service.

The risk management approach across Africa is not as mature compared to other areas of the globe, for example North America and Europe, and this is due to the size of the economies, market maturity and available skills. The development of the continent's digital economy has increased fundamentally over the past few years; however, technology and infrastructure have not matched this business growth. South Africa is an outlier in this case however, with a more robust underpinning connection backbone, and multiple service providers using different wide-area routes, as well as a high level of digital education for technical engineers and internet users alike.

Organisational Approach to Digital Risks

Technology underpins all digital client channels; however, risks should not be siloed around technology alone. Risk management should be fluid enough to change as technology changes. It may well take a large breach of someone's digital channel before risk frameworks are thoroughly re-evaluated to truly consider the changes demonstrated by the digital economy.

Digital channels are becoming increasingly important to organisations, however the level of risk management maturity at an executive level is not always adequate. As an example, for a client to access a digital channel, multiple service providers pass this data along a chain before it reaches the client, and organisations have very little insight into the risk management that these service providers enable. If a business to business internet service providers' service is unavailable, the reputational risk to their business client may not be high because they could be the only service provider in that location. However, the end clients' experience of a lack of online service could well increase the reputational risk of the business providing the service to the client, even though they do not have much control over the cause or the outcome.

Digital risk management across sub-Saharan Africa is a relatively new concept, especially because the digital economy has only arisen since the adoption of

mobile forms of communication that have enabled digital technology adoption. Sub-Saharan Africa also never had to manage the digital risks of the migration from analogue telephone systems to mobile solutions like countries across Europe and North America, so have experienced less transformation of underpinning technology.

The client experience differs dependent on the region in which they are located, and this is based on the quality of network infrastructure in those countries and regions. This is similar across industries as there are relatively few internet providers across sub-Saharan Africa. Although the move to fibre-enabled digital channels is creating certain technology challenges, for example, the upgrade of network technology within organisations to utilise fibre-optic based connections rather than older copper ADSL hardware, many of these challenges are self-perpetuated by certain large organisations. Not all organisations have these issues because of more streamlined technology designs, and removal of legacy technology environments. It is important to rationalise the number of technology systems that large corporates use to, not only improve availability of digital channels to clients, but by creating a less complex architecture, the inherent risks are reduced.

The impact of technology issues on profitability of digital channels

Internet Access Costs

The costs of internet access in first-world countries is generally much cheaper than in sub-Saharan Africa, and in many cases, the higher costs across the continent can be a barrier to entry into the digital economy for small- and medium-sized enterprises. These high costs often also shift the focus away from mitigating and managing risks before they become issues, where teams focus on restoring service to ensure the channel is available. These costs differ across regions and countries, however are still significantly higher than in first world countries.

Economic Growth

The impact that technology outages have on organisational profitability has reduced significantly over the past few years as the stability of technology has improved at both a macro and micro level. This can be quantified by utilising cost-to-income ratios as technology spend in most organisations is relatively high in comparison to other operational expenditure.

Improvements in technology across sub-Saharan Africa is lagging somewhat behind the potential for new business opportunities, so many organisations must rely on other ways of connecting with their clients to do business. However, for organisations that only provide digital channels, there is a direct financial impact from internet instability.

For example, M-PESA, Africa's first mobile money platform, which was launched by Safaricom in Kenya in 2007. If this service is unavailable, users cannot transact and therefore cannot operate. Customers in Africa are not ready for a purely digital experience; therefore, many client offerings are both digital as well as physical.

Revenue Generation

There are still multiple ways for organisations to continue to make revenue if their digital channels are not available because of internet connectivity issues. An example of this is that many digital banking channels are not consistently available, however banking revenues are still growing year-on-year across sub-Saharan Africa because clients can utilise their branch networks to initiate transactions if digital channels are unavailable. Banks are now attempting to change this inherent culture of clients utilising branches as the cost of real estate is relatedly high. However, until the digital channels are consistently available, and improvements in digital education are affected, this behaviour will not change.

The effort of technical teams constantly resolving latent technology breakdowns, like network outages stopping clients from accessing digital channels, also diverts key resources away from focusing on new value-added opportunities and revenue streams within the digital space. An example of this is shown in the release dates of mobile banking applications for two large pan-African banks.

Standard Chartered released their mobile application in June 2016, while Standard Bank only released their version in 2017. This was later because Standard Bank's approach to underlying network connectivity differs from Standard Chartered. Certain internet service providers provided an inconsistent service to Standard Bank, and therefore an inconsistent client experience.

To capitalise on these new revenue streams, organisations need to be first to market with new client offerings, especially in today's digital economy where millennials dominate the landscape, and are always looking to utilise the newest technology innovations. Organisations may well be improving revenue despite digital channel outages, however the revenue growth could have been higher if the client experience was more consistent, and the manual exercises performed to resolve issues then reduces the time for those employees to generate new value streams.

Risk Categories Related to the Digital Economy

Although cyber security risks are the most prevalent current threats to digital channels, financial risks are becoming ever more important. A prime example of these financial risks that were not evaluated and correctly mitigated recently was during the black Friday sales in South Africa in November 2017, where major e-commerce sites including online retailer Takealot, online fashion store Superbalist.com and online electronic store Dion Wired were unavailable because of the volume of e-commerce traffic. Whenever a client cannot connect to a digital channel, there are measurable revenue losses that can be applied to these times of unavailability.

The impact of network unavailability will become more and more critical for the client experience, and improvements of networks will drive business growth. If countries like the DRC have issues with underlying network technology, will the online revenues justify the potential risks of operating in this country? An initial business case should include a digital risk assessment to quantify profitability of a potential venture.

Reputational Risk

Digital transformation from manual to online channels also comes with intrinsic reputational risks, especially with the rise of social media as the de facto platform for unhappy customers to vent their frustrations. Strong cybersecurity governance, incident management strategies and good communication play a substantial part in reputational damage mitigation. There is a direct correlation between underlying network issues and a client's perception of online platforms if the platform is not available. Every network issue impacts the client's experience, and the reputational risk of having a poorly functioning digital channel could potentially reduce the client base of an organisation by more than just the client numbers directly impacted by the outage.

Many organisations in the digital economy have very similar competitors, and if one's digital channel is unavailable online then it is relatively easy for clients to purchase the same goods or services from a competitor. Outages and service interruptions stop clients using their channel of choice, and a competitor then becomes that de facto channel of choice.

Consistent service directly equates to business retention, this is important because 80% of an organisation's future revenue will come from just 20% of their existing customers (Jao, 2014). As products or services across industries can be relatively similar, the way that organisations stand out is in the way they service their clients. Offering better or more complex products may not be what clients want, or need, and although this offering may seem better from an internal viewpoint, customers may well be looking for a simpler product that is easier to use or purchase. The revenue generated from client retention is often higher than revenue from clients who purchase once-off, and then utilise a competitor for a follow up purchase because of a bad client experience.

Risk management frameworks in the digital economy

Risk Evaluation

The purpose of risk management is not always well understood, especially the fact that risk management is primarily a driver to identify and harness opportunities. Not all risks should be mitigated because then potential

opportunities may well be mitigated along with them. Many organisations recognise the growth and performance improvement opportunities that an expanded approach to risk management can provide, and there is currently a drive to educate teams on the importance of risk evaluation to help enable risk practitioners to become business value providers, rather than gatekeepers of progress. This approach is called risk-enabled performance, and is about creating tangible value where organisations can focus on ambiguity holistically, rather than classifying risks individually.

Theoretical risk analysis is quite often time consuming and may not be valid in real life situations, especially when risk analysts rely on historical data only, rather than emerging trends and predictive approaches to get a full view of a risk profile. It is important to understand what to protect and defend, and what risks to harness into new opportunities. The current process of risk management is more reactive than proactive, and often only reviews the effects of an issue after the fact, to mitigate the reoccurrence of a similar issue. Risk frameworks do not clearly define how to manage risks proactively, making it difficult to manage holistically.

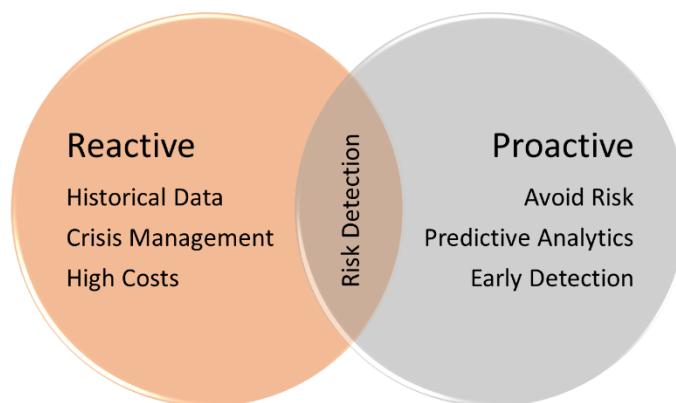


Figure 9 - Holistic Risk Detection Approach

Organisations should be re-evaluating the way they manage digital risks, as the entrenched methods often become more of an operational tick-box exercise. Risk should not be managed based on a standard risk profile, but should be driven by the organisation's strategy. This new approach should begin with the strategy,

overlaying potential threats that could affect this direction, and then attempt to manage these holistically. Rather than basing risk strategies on the default risks provided by regulations, organisations should focus on how this risk could affect the client, and what actions to take to mitigate this.

Risk Management Application

The underlying principles of risk management have not changed for some time, and should not change fundamentally into the future, however the application of these principles needs to change as technology changes. The digital revolution has been progressing for well over 15 years, and mobile channel digitisation is advancing rapidly.

Organisations should acknowledge that everyone and everything is moving into a digital economy, so organisations' philosophies and strategies need to change to harness the power of digitisation. This includes changes to operating models, as well as product offerings that enable improved risk education, as it is clear that not many people understand the definition of what a risk truly is.

Risk frameworks are not inherently obsolete, but rather the application of these frameworks within organisations may be. Client access channels may change, however the cores of processing systems have not changed all that much over time, so digital risks should focus on cyber security threats that have the potential to attack from the channel entry points. There will always be inherent risks that are not going to be successfully mitigated, but the appetite for risk should be defined to understand if the risk will be harnessed or if it is one step too far for an organisation to effectively control.

Africa's Revenue Potential

As organisations focus increasingly on the digital economy, the management of risk becomes a key factor in protecting revenue. Many people underestimate the size of the potential for business opportunities across sub-Saharan Africa, as well as the number of potential clients, which, when combined, produce significant opportunities to improve revenues.

To manage digital risks more effectively, many organisations build in increased safeguards in technology, rather than trying to improve infrastructure and lobby governments to improve underlying services, like improved fibre-optic infrastructure. Organisations should take a more holistic approach to improving African economies, which naturally mitigate risks for the greater public and help to improve economies and the GDP of the countries, rather than an internal focused view of the organisation only. This approach is also in line with the changes in the socio-economic fabric that new generations, like millennials, find important.

Backwards Looking

Risks that organisations manage impact both the organisation and the clients they service, especially because if clients have a negative experience, the reputational risk to the organisation is high, as previously discussed. Predictive and real-time data analysis could help with risk identification; however, the principles of risk governance do not need radical changes. Governance of risk is crucial for senior management to understand how they want to manage risk, are the controls in place appropriate, and are the customers adequately protected?

Because access to digital channels is becoming easier for clients, so digital security becomes more difficult to maintain. Traditional risk frameworks are not keeping pace with technology changes and potential threats that malicious individuals pose to organisations that have digital channels available to clients. This lag is in fact causing increased risks to the digital economy, rather than effectively mitigating and reducing risk levels.

Risk frameworks are still based on analysing historical data, rather than predictive analytics providing multiple possible future scenarios. Organisations that operate across multiple countries within sub-Saharan Africa should identify certain minimum technology standards across countries and regions. For example, similar standards that apply to technology in advanced countries, like South Africa and Kenya, should be applied to other countries, which can effectively mitigate certain entrenched digital risks.

Practical Examples

An example of where current risk management frameworks are not adequate includes guarantees that financial institutions issue between sellers and buyers of goods or services. As these products become digitally enabled, the digital risks become even more prevalent because of the increasing amounts of money involved, as well as the diverse country risk profiles across sub-Saharan Africa.

Another well-known example is the decline of Kodak. They did not manage their digital risks correctly and although they utilised industry-standard frameworks, they still went out of business, because in their view, digital photography would never replace the tried and tested industry standard of film. The risk identification and mitigation frameworks did not help Kodak to correctly identify the potential opportunity of digitisation and the risk of not having an adequate strategy to take advantage of this opportunity. Ironically, the very risk framework that was meant to mitigate the strategic and operational risks of the organisation, played a major role in its downfall.

Alternative solutions to managing digital risks

Risk Framework Inadequacies

Current policies and frameworks are not adequate to manage risks, let alone digital risks. Policies tend to align to governance rather than applying to fit-for-purpose, real-life situations, and are often rules based without any strategic intent. There is an opportunity to review current risk methodologies because these methodologies generally try to isolate risks across the landscape to ensure they can be quantified and mitigated effectively. We are also measuring and monitoring the incorrect metrics.

Risk frameworks and methodologies were designed for a manual analogue world, and we are attempting to apply them to the digital world. The unavailability of digital channels has a greater impact than it did before because of the number of clients using these digital channels, which has the potential to increase the impact of reputational risk, and this could be managed differently.

As an example, financial services organisations lease point of sale (POS) devices to retailers, and these devices were historically connected directly via local telecoms companies, which provided an average availability of approximately 70 per cent. Advances in technology have allowed new devices that have multiple connection options including mobile and wireless, which has improved POS availability by as much as 25 per cent.

Outdated Practical Application

Current risk frameworks are tried and tested, and should continue to be used as a base for analysis. However, traditional risk analysis has potentially become a tick-box exercise to satisfy governance rather than a true risk review, and real-life application.

Unless the risk function is skilled correctly within organisations, it will never be adequate to improve the service offered to other business units. Risk practitioners need to update their skills to have a better understanding of digital solutions, and to strengthen their partnership with technical teams.

Technology is moving at such a rapid pace, that application of risk methodologies is becoming outdated quickly. Consequently, updated risk applications are required to close the gaps created by improvements in technology, and the possibility of a new risk dimension as an addition to traditional risk management frameworks should be considered to manage digital risks holistically.

Risk management practitioners are often isolated, and not embedded within technology teams. Organisations should be looking for risk analysts with updated skillsets who understand the digital economy. The risk officer of the future should include technology and digital disruption understanding, rather than traditional risk analysis approaches only. Digital transformations in risk analysis are creating concrete business value propositions by improving the efficiency and the quality of risk based decisions. An integrated, digitised risk function also provides better monitoring and control and more effective regulatory compliance.

Technical understanding is becoming ever more important for leaders of the future, where most organisations are fast becoming technology companies,

rather than an industry split of organisations. An holistic approach to risk management can assist organisations in growing their worth, reducing the economic impact of risk, and assist in optimising processes and strategic goals.

Organisational Changes

Digital risks should be managed at an organisation's board level, demonstrating this holistic approach. Rather than isolating potential risks, these risks must be quantified correctly in terms of the strategic opportunity. Getting the right level of focus across the organisation to quantify and resolve issues effectively is critical to improving current risk management methods. This is the first step in changing mind-sets and driving the right behaviour, and by constantly reaffirming that risk is here to stay, organisations can then change their approaches to dealing with new and inherent digital risks.

Risk management should not only be viewed from the perspective of negative impact when there is a failure to protect adequately against changes in the environment, but the perspective needs to include the negative impact where there is a failure to take advantage of opportunities of the environment.

At the lower levels of the organisation, risk managers should form part of the technical delivery teams so they can understand the digital solutions, which could enable a move toward real-time risk management. This will enable risk practitioners to deploy frameworks and tools as a fully embedded service into technology teams, and can enable technology teams to be cognisant of potential threats and to design their solutions accordingly.

In addition, data governance should be factored in to be taken as seriously as digital threats. Many regulations around data are being drafted to allow an additional layer of client protection, and need to be considered in changing risk analysis.

Holistic Approaches to Risk Analysis

Scenario analysis is a new and informed way of managing technology risks; however, this still does not take an holistic view of risks across the digital

economy. Many organisations are attempting to change the way they manage risks with customised risk frameworks and new risk practitioners' who better understand the digital economy.

Technology advancements should be utilised rather than ignored to identify possible future risks that have not emerged from historical data analysis. Predictive analysis is now being used to make an educated decision on what could possibly affect digital channels in the future, by generating multiple future-based scenarios.

An holistic risk profile of both historical challenges and future scenarios provides a more informed risk profile, and these latent risks could be mitigated prior to them becoming a serious threat. The current silo approach to risk analysis is not the most effective approach to risk management to effectively understand and mitigate digital risks. This means that risk analysis skills need to change to become more technology focused.

Changes to current risk management frameworks to better manage these emerging digital risks

In general, organisations risk mitigation efforts have increased in the past few years, based on the increasing threats affecting digital channels. However, risk management practices are outdated, and updates or new approaches to frameworks and methodologies are required to manage digital risks more effectively.

Current risk management frameworks can be altered, to include a digital-risk specific section in each risk category. Alternatively, new frameworks should be considered that help analyse real-time threats, and should be capable of handling digital threats as quickly as possible.

Updated Risk Frameworks

Potentially, there is an opportunity to create new risk frameworks rather than building on current frameworks, however many large organisations may well

resist new approaches because they then need to admit that the old way of managing risks is no longer valid.

New risk approaches should start with the business strategy, and align this to understanding the areas of potential losses of income. Once this is understood, a strategic approach to either improving digital services to clients, or increasing the cost of goods and services to price in for this loss can be implemented accordingly. However, the second option is not client-centric and is not a truly viable solution to growing a business sustainably over the longer term.

It is already difficult enough to implement an effective, standard risk management framework in an organisation, so it would be quite challenging to attempt to change an already entrenched approach to risk management.

Technology Utilisation

The underlying theory inherent in risk approaches is potentially becoming redundant by the time the work is completed to manage the risks because of the speed at which technology is changing. Many industries' largest risk factor is, in fact, their continued existence, and the speed at which technology changes is allowing disruptors into most industries, who utilise agile techniques and can tap into the market changes faster than traditional large organisations.

The more digitised economies across sub-Saharan Africa become, the more data is available for systems to store and consume. Analytical technology can then utilise this data to both analyse historical data and apply it to predictive modelling that utilises this data to propose a view of what may happen in the future.

If one brings these two approaches together, then organisations can improve on their overall risk profile. The world is not completely digital yet however, so measuring both approaches can help manage risks across digital and other channels.

Predictive analytics helps harness technology to manage technology risks more effectively. An example of this is how cybercrime evolves so fast that historical

data will never be able to help mitigate future risks in this category because the data is inherently obsolete by the time it is reported.

Risk frameworks should include a principle-based approach rather than isolating risk categories, especially because, if risks do not fit a category, how do you effectively manage them? Digital risks often span across the organisation and across multiple risk categories, so rather than box risks into a sub-category, the question is what action plans are in place to either mitigate or harness them?

There has been an update to the COSO framework released in 2017, which approaches risk management from a strategic view. The view is that all risk approaches should be data-led rather than qualitative, and specifically accommodate emerging technologies and the propagation of information and analytics in supporting decision-making.

Holistic Risk Profiles

If traditional risk management continues to focus on historical trends and data, rather than identifying possible opportunities looking forward, the offering to clients will no longer be relevant and without clients, there is no revenue.

As an example, block chain technology enabling crypto-currency and mobile payments that do not have as strict regulations are some of the key emerging issues with which financial institutions need to contend.

Current risk frameworks are designed to focus on historical data analysis, they do not, however, have the ability to look at predictive analysis to complete a risk profile. There is the possibility of integrating both historical and predictive data analysis to give organisations a better view of the risk profile.

Summary of the results

The key findings that have been discussed in this section confirm the fact that there are significant challenges in how adequately current risk management guidelines cover digital problems that have arisen out of the digital economy, specifically within sub-Saharan Africa.

In the next chapter, an examination of the data collected from semi-structured face-to-face interviews is provided, grounded on the information in chapter four.

DISCUSSION OF THE RESULTS

Introduction

The idea of risk management might at first seem straightforward, namely that the risks are identified and quantified correctly, and following this, mitigation actions are put in place to manage these risks effectively. However, risk management, especially in the digital economy, is multifaceted and this was established in the review of the literature in chapter two.

This is further substantiated by the research results from this study, which showed that respondents felt that the digital economy is progressing so rapidly that current risk management approaches are swiftly becoming outdated, and do not adequately consider the impact of technology outages on digital customer channels. The conclusion provides an insight of the deductions from the research and where appropriate, links the literature to the study conclusions.

Discussion

Results Explanation

Although the findings were consistent across all respondents, there were certain responses that differed slightly in their approaches. Most respondents understood that current risk approaches are based on an historical view of data, and their opinion was that this is not holistic enough to generate a true, complete risk profile. To get this holistic view, technology should be harnessed to enable predictive analytics to provide multiple future scenarios.

However, some of the respondents were of the view that current risk frameworks and methodologies are still effective, the only change that is required is in the way that we apply them at a practical level. The theory of risk management does not need to change just because new risk themes are emerging across economies. Organisations should no longer approach risk analysis as a tick-box exercise, but rather from a strategic approach to harness additional opportunities.

References to Previous Research

(van Wyk, 2015)'s analysis highlights that Africa has a lower percentage of early-stage risk mitigation, talks directly to the lack of adequate risk education across sub-Saharan Africa and directly corresponds to the number of digital risks experienced in this part of the world compared to more developed economies. Passenheim (2010) discusses how many organisations still look at risks in isolation and this requires a more holistic approach, because digital risks can span the entire breadth of an organisation and cannot always be isolated and controlled effectively. While this level of specialisation is essential to manage specific risk factors appropriately, compartmentalising risk managers can stifle the organisations' best, holistic approaches to risk management (Layton, 2007).

(Seck, Belai, & Nwuke, 2014) argue how e-commerce channels are subjected to technical risk factors that other channels are not, and how cybercrime is an increasing threat worldwide, but growing at a more rapid rate across Africa than in any other region of the world (Symantec Corporation, 2013), returning finally to (Folpmers, 2016), who states that current risk taxonomies do not address new risks, and (Liew, Bellens, & Webster, 2016) who detail how the management of digital risk is becoming more important because threats are impacting business profitability. Although this aligns somewhat to the research concluded in this report, it does not continue to describe how to remedy this issue, and does not discuss the opportunities around real time and predictive risk analysis to enhance the process of risk analysis.

Deduction

While these results focus on sub-Saharan Africa, the recommendations provided can be applied generically to the digital economy worldwide, because the potential threats are similar. However, because of the rate of growth of this sector across sub-Saharan Africa, it is fundamental that these recommendations are put into practice in this region sooner rather than later.

The digital economy in sub-Saharan Africa is still in its infancy when compared to other regions of the globe, for example, North America, Europe and China.

However, the exponential growth that has been enabled by the advancement in technology (both mobile for internet access and infrastructure-wise for enablement) leaves sub-Saharan Africa at a much higher risk to digital threats because education focused on the digital economy is not as advanced as in other areas of the world.

Digital channels are focused on customers, as without them there is no requirement for a channel of this nature, or in fact, for a business. The digital drive of many organisations often begins with improving internal productivity, focusing primarily on improving effectiveness and reducing costs and inherent risks. Where this fails to intersect with the client experience however, is the progressively sophisticated customer expectations of a personalised customer experience. The difficulty many organisations face is how best to convert their systems to both service the client's needs, as well as delivering this securely in a real-time environment.

Risk and compliance divisions can often end up as gatekeepers instead of partners during the development of innovative ideas within organisations, and requires new approaches to become advisors to help analyse risks and provide viable solutions. This requires improved technology risk analysis tools that can produce fluid frameworks and guidelines and establish improved controls to protect the process. The current culture of control requires a change so that the decision of whether to take a risk becomes collaborative.

Digital risk is a relatively new dimension for organisations to manage, and is becoming increasingly important given threats like technology outages, disintermediation, cybercrime and data loss. The guidelines and frameworks that have safeguarded organisations to date may not be adequate to address these new risks in the future. Digital risk management should form part of an overarching technology risk framework, and include standard technology practice analysis including architectural design, access, data and vendor management, and service availability in conjunction with cyber security and reputational risk metrics to ensure a more holistic approach to this type of risk analysis.

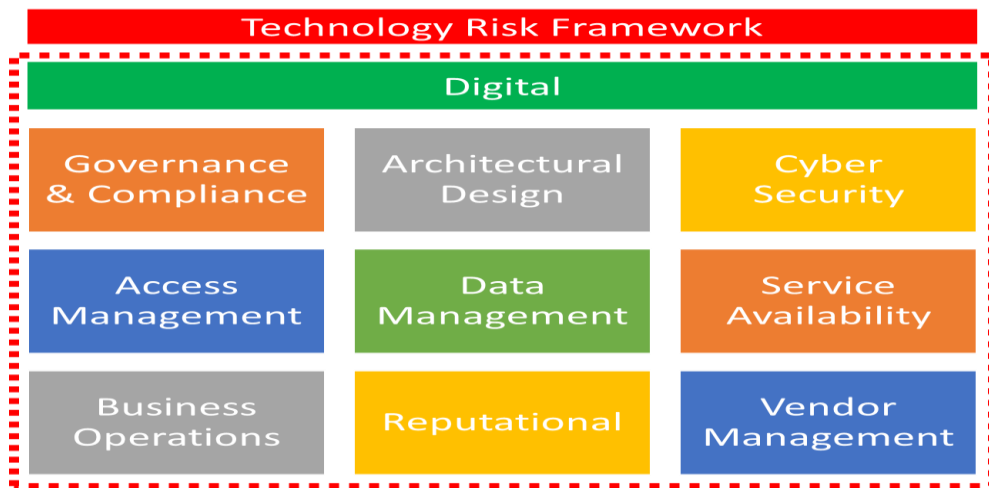


Figure 10 - Technology Risk Framework

Conclusion

Based on the content of the interviews conducted by the author, the general view is that current risk management frameworks are not adequate to cater for emerging digital risks that relate to inconsistent internet connectivity, potentially impacting on e-commerce and the digital economy.

Three main themes on how to improve on current risk management guidelines that do not explicitly cover digital risks that have arisen out of the digital economy in sub-Saharan Africa, emerged from the interviews conducted:

1. These risks can be adequately managed by enhancing current risk frameworks to include a digital sub-section within each risk category. By following the current risk methodologies with this updated framework, these risks can be adequately mitigated.
2. Current risk management frameworks do not cater for emerging digital risks like inconsistent internet connectivity, especially as the frameworks are outdated and do not change as quickly as technology, therefore new methods of managing these risks are required.

3. Current risk management frameworks have been successful for a long period of time and do not require any changes. However, they should be combined with predictive analytics to broaden the approach to managing risk by providing a more holistic approach to risk management.

CONCLUSIONS & RECOMMENDATIONS

Introduction

This research paper was intended to understand whether current risk management approaches adequately mitigate inherent risks within the digital economy in sub-Saharan Africa and may either require a review of current risk management approaches, or an updated risk framework.

The conclusions focus on three consolidated views on how risk management could be updated to improve the current methodologies, which, if implemented correctly, could help reduce the inconsistent client experience of digital channels, improve organisations' revenue because of an improved service and additional geographical reach, and in turn, improve economies of countries within sub-Saharan Africa.

Conclusions of the study

Summary

Risk management in the digital era is not about management at all, but more about how organisations navigate risks. In this fast-paced environment, many organisations do not have time to effectively manage risks, however navigating risks effectively to harness opportunities in real time has the potential to improve organisations revenues, the economies to which they belong, and ultimately the lives of Africans on this continent we call home.

This study concluded that risk management, as it stands today, does not adequately deal with the constant emergence of new digital risks including inconsistent internet connectivity, and either new or improved risk management frameworks may well be required to manage this threat effectively. By the time we understand the risks well enough to manage them, the risks themselves have changed. It would be far more beneficial for risk frameworks to provide tools and guidance on how to best navigate these risks than to try to manage them.

Based on the content of the interviews conducted by the author, the general view is that current risk management frameworks are not adequate to cater for emerging digital risks potentially impacting e-commerce and the digital economy. The author has not attempted to redefine the process for analysing risks in this section.

Updated Risk Framework

In the diagram below, the author has encompassed each of the approaches that the respondents have discussed that form part of technology risk, and grouped each of these items into a framework that specifies the types of risks of which organisations should be cognisant when analysing technology risks. Digital risks are placed specifically in this framework to be overarching across the spectrum, as these risks cannot be specifically isolated and may encompass one or many of the other risk definitions.

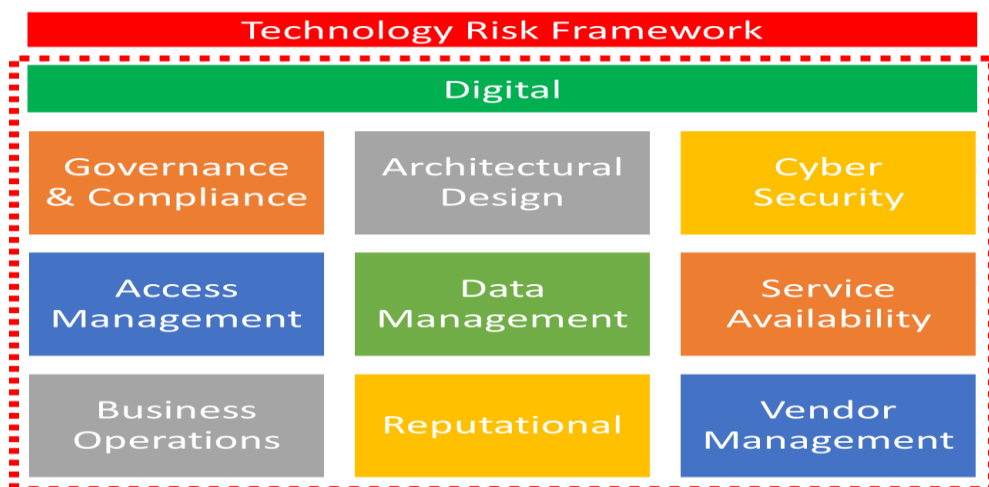


Figure 11 - Technology Risk Framework

Predictive Analytics Approach

Alternatively, current risk management frameworks do not cater for emerging digital risks, especially as the frameworks are outdated and do not change as quickly as technology, therefore new methods of managing digital risks are required. In the diagram below, the author has provided a graphical view of the process of predictive analytics, which is defined as the branch of advanced

analytics used to make predictions about future events (Predictive Analytics Today, 2018). Using predictive analytics to analyse data and provide multiple scenarios around what risks may become prevalent, could provide the right information prior to an event to allow organisations to effectively mitigate such a threat. The diagram below shows the standard pattern a predicative analytics model follows to ensure the correct data is utilised to drive the relevant predictive models.

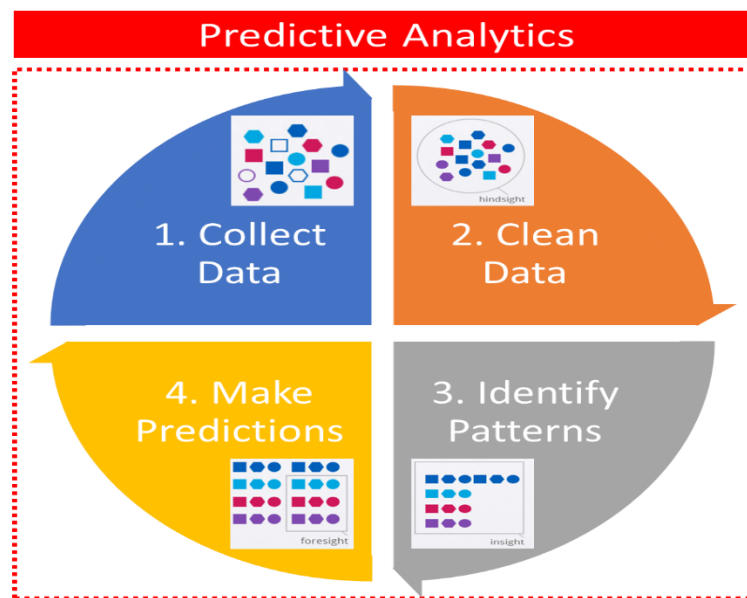


Figure 12 - Predictive Analytics Data Flow (Predictive Analytics Today, 2018)

Consolidated Approach

The combined view of the previous two approaches is that while current risk management frameworks have been successful for a long period of time and, although they do not require fundamental changes, the way we apply them should change. The author has applied the previous two solutions into a consolidated approach (depicted in the diagram below) that joins current risk methodology approaches to analysing historical data, with a predictive approach to give a more holistic view of technology risks and how best to manage them.

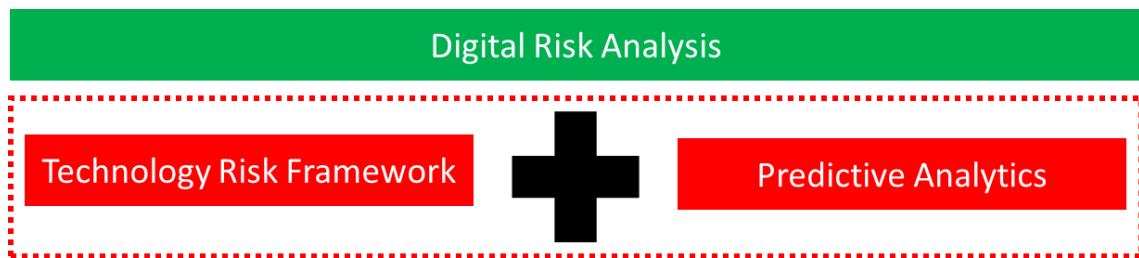


Figure 13 - Holistic Digital Risk Analysis

Along with this combined approach to analysing risks, the structure of organisations need to change to ensure risk practitioners are embedded in business units and technology teams. By doing this, the teams can then focus on the following four questions as a basis for analysing and understanding technology risk:

1. What is going on around us?
2. What are we trying to achieve?
3. What could go wrong with our changes?
4. What should we do about it?

Recommendations

Summary

The recommendations include a practical approach to updated risk management methodologies, to understand the exact point of failure of the underlying frameworks. Once this is understood, then a new framework can be designed with the help of technologists, information technology security analysts and risk management practitioners.

Recommendations

1. Risk management approaches should include the possibility of predictive analysis to make an educated decision on what could possibly affect digital channels in the future, rather than only analysing historical data to build a risk model. Predictive risk management requires a flexible, responsive

organisation, which means that outdated business operations have become a genuine threat to the very existence of an organisation.

2. Standard country and regional risk profiles should be available for new entrants into the market to easily access, as this should help the markets identify and mitigate potential risks earlier and more effectively. This collaboration is one of the many ways that the digital economy could get ahead of the cyber security threats.
3. Risk management practitioners should be embedded within business units, and technical delivery teams so they can understand the digital solutions and risks and manage risks in real time. Risk management cannot be all-inclusive if it is limited to isolated silos within an organisation. Threats can arise from many angles, and these threats cannot always be isolated, especially from a digital standpoint where they often have the potential to affect the entire breadth of an organisation.

Suggestions for further research

Further research should be conducted on the use of robotics and artificial intelligence technology, focused on predictive analytics to begin to actively monitor risks across sub-Saharan Africa. This technological approach can begin to build up the necessary information to predict, with certain levels of certainty, what emerging risks are on the horizon for organisations within the digital economy, and how best to mitigate or manage these risks. The use of technology to actively monitor digital risks is the ideal solution for technology-based risks that emerge faster than humans can actively monitor and evolve to mitigate effectively against them.

How can digital education be placed at the centre of school curricula across sub-Saharan Africa? To achieve the integration of Africa into the world economy, the mastery of these technologies is essential to not only progress the digital economy across Africa, but for the role players to adequately understand the risks these channels possess, and how best to manage them. This approach identifies

other latent issues in the general quality of education across most of sub-Saharan Africa and is out of the scope of this study.

REFERENCES

- Bekele, D. (2017). *Internet Shutdowns Are Not a Solution to Africa's Challenges*. Geneva: Internet Society.
- Belson, D. (2017, November 28). *The Migration of Political Internet Shutdowns*. Retrieved from Oracle: <https://dyn.com/blog/the-migration-of-political-internet-shutdowns/>
- Boehm, B. (1989). Software risk management. In C. Ghezzi, & J. A. McDermid, *Lecture Notes in Computer Science*. Berlin: Springer.
- Busha, A. (2014, November 13). *Growth of E-Commerce in Nigeria*. Retrieved from <https://mobilemediainfotech.wordpress.com/2014/11/13/600/>
- Chinn, M. D., & Fairlie, R. W. (2010). ICT Use in the Developing World: An Analysis of Differences in Computer and Internet Penetration. *Review of international Economics: Volume18 Issue 1*, 153-167.
- CNBC Africa. (2017, January 4). *M-pesa has completely transformed Kenya's economy, this is how....* Retrieved from CNBC Africa: <https://www.cnbc africa.com/news/east-africa/2017/01/04/mpesa-economic-impact-on-kenya/>
- Cohen, L., Manion, L., & Morrison, K. (2000). *Research Methods in Education*. London: Routledge Falmer.
- Committee of Sponsoring Organisations. (2004). *Welcome to COSO*. Retrieved from Committee of Sponsoring Organisations: <https://www.coso.org/Pages/default.aspx>
- Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management - Integrating with Strategy and Performance*. Committee of Sponsoring Organizations of the Treadway Commission.

- Cooper, D. R., & Schindler, P. S. (2006). *Marketing Research*. London: Macmillan.
- Dahir, A. L. (2017, January 13). *If you want affordable internet in Africa, move to a country on the coast*. Retrieved from Quartz Africa: <https://qz.com/africa/884072/if-you-want-affordable-internet-in-africa-move-to-a-country-on-the-coast/>
- Dahir, A. L. (2017, November). *Internet shutdowns continue to cost Africa's economies*. Retrieved from Atlas: <https://www.theatlas.com/charts/S1LpT9ci->
- Denyes, L., & Lonie, S. (2016). *Digital Financial Service and Risk Management Handbook*. Ontario: The MasterCard Foundation.
- Denzin, N. K., & Lincoln, Y. S. (2005). *The SAGE Handbook of Qualitative Research*. Los Angeles: SAGE Publications.
- Deutscher Corporate Governance Kodex. (2017). *Deutscher Corporate Governance Kodex*. Retrieved from Deutscher Corporate Governance Kodex: <http://www.dcgk.de/en/home.html>
- Dhliwayo, J. (2005). Developing a Fibre Optic Backbone for Africa. In S. Danofsky, *Open Access for Africa: Challenges, Recommendations and Examples* (pp. 122-133). New York: The United Nations Information and Communication Technologies Task Force.
- du Plessis, M., & Boon, J. A. (2004). Knowledge management in eBusiness and customer relationship management: South African case study findings. *International Journal of Information Management: Volume 24 Issue 1*, 73-86.
- Ekekwe, N. (2015). The Challenges Facing E-Commerce Start-ups in Africa. *Harvard Business Review*.
- Ernst & Young. (2014). *Expecting more from risk management*. Johannesburg: Ernst & Young.

- Export.gov. (2017, July 20). *Congo, Democratic Republic - Telecommunications*. Retrieved from Export.gov: <https://www.export.gov/article?id=Congo-Democratic-Republic-Telecommunication>
- Folpmers, M. (2016, October 1). *A Call to Overhaul the Traditional Risk Taxonomy*. Retrieved from Global Association of Risk Professionals: <http://www.garp.org/#!/risk-intelligence/all/all/a1Z40000003LI7sEAC/call-to-overhaul-traditional-risk-taxonomy>
- Forden, E. (2015). *The Undersea Cable Boom in Sub-Saharan Africa*. Washington: United States International Trade Commission.
- Forden, E. (2015). *The Undersea Cable Boom in Sub-Saharan Africa*. Washington DC: United States International Trade Commission.
- Gady, F.-S. (2010, March 29). *Foreign Policy: Africa's Internet Threat*. Retrieved from National Public Radio: <http://www.npr.org/templates/story/story.php?storyId=125297426>
- Goldstuck, A. (2012). *Internet Matters: The Quiet Engine of the South African Economy*. Johannesburg: World Wide Worx.
- González, F. (2005). Bank regulation and risk-taking incentives: An international comparison of bank risk. *Journal of Banking & Finance: Volume 29 Issue 5*, 1153-1184.
- Hsu, D. (2016, April 5). *Meet Africa's First Tech 'Unicorn' - Are More to Come?* Retrieved from Wharton University of Pennsylvania: <http://knowledge.wharton.upenn.edu/article/meet-africas-first-tech-unicorn-are-more-to-come/>
- International Organization for Standardization. (2009). *IEC 31010:2009 Risk management - Risk assessment techniques*. Retrieved from International Organization for Standardization: <https://www.iso.org/standard/51073.html>

- Internet Online. (2017, November 2017). *#BlackFriday: Online stores like Takealot, Superbalist crash*. Retrieved from Internet Online: <https://www.iol.co.za/business-report/blackfriday-online-stores-like-takealot-superbalist-crash-12138109>
- Internet Usage Statistics. (2017, June 30). *Internet Usage Statistics*. Retrieved from Internet World Stats: <http://www.internetworldstats.com/stats.htm>
- Jao, J. (2014, November 19). *Why Customer Retention Is King: The Evolution Of Retention Marketing*. Retrieved from Forbes: <https://www.forbes.com/sites/jerryjao/2014/11/19/why-customer-retention-is-king-the-evolution-of-retention-marketing-part-1/#3c722f41186b>
- Katz, R. (2012). *Impact of Broadband on the Economy*. Geneva: International Telecommunication Union.
- Kende, M. (2017). *Promoting the African Internet Economy*. Reston: Internet Society.
- Kossovsky, N. (2014, April 1). *How to Manage Reputation Risk*. Retrieved from Risk Management: <http://www.rmmagazine.com/2014/04/01/how-to-manage-reputation-risk/>
- Kshetri, N. (2007). Barriers to e-commerce and competitive business models in developing countries: A case study. *Electronic Commerce Research and Applications: Volume 6 Issue 4*, 443-452.
- Kshetri, N. (2018). Rural e-Commerce in Developing Countries. *IT Professional: Volume 20 Issue 2*, 91-95.
- Kvale, S. (1996). *Interviews*. London: SAGE Publications.
- Lakner, C., & Milanovic, B. (2013). *Global Income Distribution From the Fall of the Berlin Wall to the Great Recession*. Washington: The World Bank.
- Lark, J. (2015). *ISO 31000 A Practical Guide*. Geneva: International Standards Organisation.

- Layton, M. (2007, March). *Traditional Risk Management Inadequate To Deal with Today's Threats*. Retrieved from International Risk Management Institute: <https://www.irmi.com/articles/expert-commentary/traditional-risk-management-inadequate-to-deal-with-todays-threats/>
- Liew, N., Bellens, J., & Webster, I. (2016). *Managing change and risk in the age of digital transformation*. Singapore: EY.
- Madkour, M. (2018, June 9). *What will drive Africa's digital economy*. Retrieved from IT News Africa: <http://www.itnewsafrica.com/2018/06/what-will-drive-africas-digital-economy/>
- Many Possibilities. (2016, November 1). *African Undersea Cables – Interactive*. Retrieved from Many Possibilities: <https://manypossibilities.net/african-undersea-cables-interactive/>
- Matinde, V. (2017, January 16). *Africa 2017: Smartphone penetration, Open Data and less online freedom*. Retrieved from IDG Connect: <https://www.idgconnect.com/blog-abstract/23175/africa-2017-smartphone-penetration-open-data-online-freedom>
- Mbarika, V., Jensen, M., & Meso, P. (2002). Cyberspace across sub-Saharan Africa. *Communications of the ACM: Volume 45 Issue 12*, 17-21.
- McCarthy, N. (2017, November 22). *The Most And Least Expensive Countries For Broadband*. Retrieved from Forbes: <https://www.forbes.com/sites/niallmccarthy/2017/11/22/the-most-and-least-expensive-countries-for-broadband-infographic/#2ab6126423ef>
- Mohammed, O. (2015, August 14). *With a billion Africans set to shop online, a new wave of start-ups is looking to cash in*. Retrieved from Quartz Africa: <https://qz.com/478714/africas-emerging-consumer-class-is-a-boon-for-the-continents-online-retailers/>
- Muhumuza, R. (2017, March 14). *African governments learn to block the internet, but at cost*. Retrieved from Phys.org: <https://phys.org/news/2017-03-african-block-internet.html>

- My Broadband. (2018, January 15). *South Africa at higher risk of data breaches, says phishing trend report*. Retrieved from My Broadband: <https://mybroadband.co.za/news/industrynews/244595-south-africa-at-higher-risk-of-data-breaches-says-phishing-trend-report.html>
- Ncube, M., Lufumpa, C. L., & Kayizzi-Mugerwa, S. (2011). *The Middle of the Pyramid: Dynamics of the Middle Class in Africa*. Abidjan: African Development Bank.
- Nkemdilim, C. (2015, February 19). *Nigeria Is Leading South Africa And Kenya In E-Commerce*. Retrieved from TechCabal: <http://techcabal.com/2015/02/19/nigeria-leading-south-africa-kenya-e-commerce/>
- Nyirenda-Jere, T., & Biru, T. (2015). *Internet development and Internet governance in Africa*. Geneva: Internet Society.
- OECD. (2014). *Risk Management and Corporate Governance*. Paris: Organisation for Economic Co-operation and Development.
- Oyelaran-Oyeyinka, B., & Adeya, C. N. (2004). Internet access in Africa: empirical evidence from Kenya and Nigeria. *Telecommunications Development in Africa: Volume 21 Issue 1*, 67-81.
- Passenheim, O. (2010). *Enterprise Risk Management*. Frederiksberg: Ventus Publishing.
- Peroni, M., & Bartolo, M. (2018). The Digital Divide. In M. Peroni, & M. Bartolo, *Multidisciplinary Teleconsultation in Developing Countries* (pp. 101-109). Cham: Springer.
- Pirner, P., & Eschner, B. (2017). *Connected Customer: Omni-channel Management in a Connected World*. London: Kantar.
- Predictive Analytics Today. (2018, January 22). *What is Predictive Analytics*. Retrieved from Predictive Analytics Today: <https://www.predictiveanalyticstoday.com/what-is-predictive-analytics/>

- PwC. (2016). *Getting the balance right*. Johannesburg: PwC.
- PwC. (2016). *King IV - Steering point*. Johannesburg: PwC.
- Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science: Volume 27 Issues 2–3*, 183-213.
- Research ICT Africa. (2017, May 23). *Data capture: South Africans not enjoying the price fall in Africa*. Retrieved from Research ICT Africa: https://researchictafrica.net/ria_rap/2017/05/23/data-capture/
- Rossmann, G. B., & Rallis, S. F. (2012). *Learning in the Field: An Introduction to Qualitative Research*. Los Angeles: SAGE Publications.
- Roycroft, T. R., & Anantho, S. (2003). Internet subscription in Africa: policy for a dual digital divide. *Telecommunications Policy: Volume 27 Issues 1–2*, 61-74.
- Seck, M., Belai, T., & Nwuke, K. (2014). *Tackling the challenges of cybersecurity in Africa*. Addis Ababa: United Nations.
- Senate and House of Representatives of the United States of America. (2002). *Sarbanes-Oxley Act of 2002*. Washington DC.
- Siemens. (2017). *African Digitalization Maturity Report*. Johannesburg: Siemens.
- Song, H., Fink, G. A., & Jeschke, S. (2018). *Security and Privacy in Cyber-Physical Systems*. Chichester: John Wiley & Sons.
- Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. *National Institute of Standards and Technology*.
- Stork, C., Calandro, E., & Gillwald, A. (2013). Internet going mobile: internet access and use in 11 African countries. *Info: Volume 15 Issue 5*, 34-51.
- Storm, L. (2017, April 3). *Negative Impact of the Internet on Business*. Retrieved from It Still Works: <http://itstillworks.com/negative-impact-internet-business-1393.html>

- Swart, A. J. (2014). *Using online assignment submissions at an open distance learning institute to predict future Internet traffic for a higher educational institution!* Nelson Mandela Bay: Southern Africa Telecommunication Networks and Applications Conference.
- Symantec Corporation. (2013). *Internet Security Threat Report 2013*. San Francisco: Symantec Corporation.
- The GSM Association. (2016). *The Mobile Economy*. London: The GSM Association.
- Trevor, M., Inglis, K., & Heard, A. (2016). *Data Center Risk Index*. Chicago: Cushman & Wakefield.
- Twinomugisha, A. (2010, May 5). *Why African Internet Bandwidth Prices Are Still High*. Retrieved from ICT Works: <https://www.ictworks.org/why-african-internet-bandwidth-prices-are-still-high/#.Wn6wvvkjG00>
- van Wyk, A. (2015). *Africa risk in review 2015*. Johannesburg: PWC.
- van Zyl, G. (2016, October 17). *Seacom cable fault hits SA internet*. Retrieved from News 24: <http://www.fin24.com/Tech/News/just-in-seacom-cable-fault-hits-sa-internet-20161017>
- West, D. M. (2016). *Internet shutdowns cost countries \$2.4 billion last year*. Washington: The Brookings Institution.
- Wolke, T. (2017). *Risk Management*. Berlin: De Gruyter.
- World Bank Group. (2016). *Digital Dividends*. Washington: World Bank Group.
- Wynne, C., Berthon, P., Pitt, L., Ewing, M., & Napoli, J. (2001). The impact of the Internet on the distribution value chain: The case of the South African tourism industry. *International Marketing Review: Volume 18 Issue 4*, 420-431.

Zittrain, J. L., Faris, R., Noman, H., Clark, J., Tilton, C., & Morrison-Westphal, R. (2017). The Shifting Landscape of Global Internet Censorship. *Berkman Klein Center Research Publication: Number 2017-4*, 17-38.