Mendel university in Brno

Faculty of Regional Development and International Studies

Promotion of Regional Development in South Africa through increasing level of Cyber Security

Diploma thesis

Supervisor of thesis:
Ing. Zbyšek Korecki, Ph.D.

Author of thesis:
Bc. Michal Haas

Brno 2016

I would like to express my acknowledgment to my supervisor Ing. Zbyšku Koreckimu, Ph.D. for his helpful and needed advices while elaborating this thesis with professional guidance. His contribution and professionalism has brought a light to my work and experience for my future life. Furthermore I would like express my acknowledgment to Sodat Software company, providing a great life opportunity for enriching my knowledge and bringing me into dilema of cyber security.

Declaration

I declare that I carried out this thesis:

independently, and only with the cited sources, literature and other professional sources.

I agree that my work will be published in accordance with Section 47b of Act No. 111/1998 Coll. on Higher Education as amended thereafter and in accordance with the Guidelines on Publishing University Student Theses.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular the fact that Mendel University in Brno has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 paragraph 1 of the Copyright Act.

Before closing a license agreement on the use of my thesis with another person (subject) I undertake to request for a written statement of the university that the license agreement in question is not in conflict with the legitimate interests of the university, and undertake to pay any contribution, if eligible, to the costs associated with the creation of the thesis, up to their actual amount.

In Brno, 20. 5. 2016

Michal Haas

Abstract

Topic of this diploma thesis is focused on cyber security situation in African Union particularly in South Africa looking and analyzing the legislative background of African Union and South Africa after introduction of African Union Convention on Cyber Security and Personal Data Protection. Legal background supported on continental level and governmental level should point on importance of this topic and encourage states bodies for action. Analysis and comments on legal aspects, suggestions and regulations introduced in the Convention together with practical examples from global environment and South Africa as well will point on opportunities in regional development consiting in this topic. In suggestion part is proposed Cyber Security Concept that is transferring general articles from African Union Convention into short guide with comments on ratified content by Member States of African Union, reviewing those points wirh our related topic and filling up missing parts based on experiences from European Union.

Keywords: Cyber Security, African Union Convention, regional development, promoting security, legal aspects in African Union, Cyber Security Concept

Abstrakt

Téma této diplomové práce je zaměřeno na situaci kybernetické bezpečnosti v Africké unii, přesněji v Jižní Africa, kdy bylo sledováno a analyzováno legislativní pozadí v Africké Unii a Jižní Africa po uvedení úmluvy africké unie na kybernetickou bezpečnost a ochranu osobních dat. Legislativní pozadí podporované na kontinentální a vládní úrovni poukazuje na závažnost v této oblasti a vyzívá státní orgány k akci. Analýza a komentáře k legislativnímu pozadí, doporučení a omezení představené v úmluvě Africké unie společně s praktickými příklady ze světového prostředí spolu s z prostředí Jižní Afriky poukazují na možnosti a příležitosti v oblasti regionálniho rozvoje, spočívající v otázce kybernetické bezpečnosti. V návrhové části je navržen Koncept Kybernetické Bezpečnosti který převádí obecné články z úmluvy Africké Unie do krátkého průvodce a návodu s komentáři na odsouhlasený obsah členskými státy Africké unie, revidující související body s diskutovanou problematikou a doplňující části na základě zkušeností a poznatků z Evropské Unie.

Klíčová slova: Kybernetická bezpečnost, úmluva africké unie, regionální rozvoj, podpora bezpečnosti, legislativní aspekty v africké unii, koncept kybernetické bezpečnosti

Table of Content

Introduction

Today society live in a environment that relies on information systems and slowly becomes fully dependent on them. Threatening of their functionality might affect its basic operational actions inside for their existence.

Abbreviation “cyber security” is relatively new term used and analyzed in last approximately 20 years. Relevance of this new phenomenon is growing in importance especially after security incident occurs. This is a typical behaviour of organizations that underestimate security challenges and afterwards pays tremendous amount of money to recover from cyber incident to default state. Importance of the whole security management concept is underlined by existence of ISO 27001 - Information security management which goal is to keep information assets secure.

The networked computer systems are accessible remotely and have become potential targets of cyber attacks which compromise the capacity to process, safeguard, communicate informational capital, intangible values and symbols, and the process of production or decision of those possessing such symbols, with implications for the security and survival of States and organizations.

By enforcing the law about cyber security was made an initial step to resolve security of information systems across private and public sectors, preserving their operating process and mainly ensuring the sensitive data in the hands of the organization

Not only the world characterized by the globalization of risks, crimes and threats to cyber security. Africa is faced with security gap which, as a result of poor mastery of security risks, increases the technological dependence of individuals, organizations and States on computer systems and networks that tend to control their information technologies needs and security facilities.

It should however be observed that most African States neither have communication tools that integrate adequate means as required to achieve or guarantee a minimum level of security, nor have the human resources capable of conceiving and creating a credible legal framework.

Today, Africa more than elsewhere in the world, should as a matter of urgency offer individuals, organizations and States measures, procedures and tools for more effective management of technological, informational and legal risks. The stakes inherent in the effective control of technological risks are extremely high, and have to be addressed globally at the international level, by taking all Member States of the Union on board the security initiative, while respecting the fundamental rights of persons and of the States.

Goals and Methodology

Goals

Intention of diploma thesis is to carry out proposal to South African government to sectors where the question of information security is relevant topic. Target for changes is related with management of human and information technology resources and information protection based on executed case studies in similar sectors on different subjects. The goal will be achieved by examining chosen parts of case studies that are set up as separate section of analytical part of the diploma thesis and its affects on the subject. Analyzed parts of the case study will point on crucial points in organization's conduction of the subject and show on alternative possibilities on management of human and IT resources with possitive outcome in increased security of information and secondary on more importantly on state's budget.

Theoretical part will cover the related regional development theories of region together and theory of cyber security that can be used to facilitate conduction of the organization and management of it's resources. It also covers re-engineering theory explaining how to keep up those standards on management still relevant to the changing environment of the organization and external threats.

Practical part will study picked up areas in case study to point on important aspects in management of information assets, framework of processes, IT resources with description of each individual topic and tools that have a great influence in securing information assets and other. Information protection in the practical part desrcibes the importance of data security and impacts on organization budget in case of loss and abusement of such data. Such examination will require use of other relevant and trustful sources to be able to exercise and demonstrate the impacts.

Methodology

Achieving the goals specified in the previous part asks for using induction and decution method while examining legal aspects to determine important articles and related information listed in the Convention. Another method used account for qualitative and quantitative scientific methods in examining case studies from cyber security environment of subjects from public, private and governmental level. Allocated information from analytical part were reconsidered and logically applied in following suggestion part to be able to carry out Cyber Security Concept for South African government with theoretical insights from the case studies and African Union Convention on Cyber Security.

1. Theoretical Part

1.1. Regional Development Theories

Relevant theories related with topic of my diploma thesis will cover a more areas at once due to complexity of this topic. On the first sight cyber security might appeal as a concept seeking only at level of security measures applied in the state to protect own land, citizens, perimeter of organizations etc. After deeper examination, it will turn in to a conclusion that cyber security is related individuals, groups, elites, organizations, politica parties, public authorities, financial insitutions and many other subjects borderless to any states, groups or individuals leaving classical obstacles irrelevant. Having any information or data allocated at one secure place preserves our comparative or absolute advatantage, competitiveness, sensitive personal information about health, financial information, framework of processes, agreements, political affiliations and other extremely important information secured from any other persons that have any fraudulent intentions with such information. Thus in theoretical approaches exists certain convergence in our examined topic.[1]

1.1.1. Location theories

One of such theory relevant to our topic is location theory, describing concentration of activities in regions and agglomerations without any importance given to geographical features.

Location theory gives regional economics its scientific-disciplinary identity and constitutes its theoretical-ethodological core. It has typically microeconomic foundations and it adopts a traditionally static approach. It deals with the location choices of firms and households. Linked with it are a varieties of metaphors, cross-fertilizations, and theoretical inputs (from macroeconomics, interregional trade theory, development theory, mathematical ecology, systems theory) which have refined the tools of regional economics and extended its range of inquiry. In microeconomic terms, location theory involves investigation into the location choices of firms and households; but it also involves analysis of disparities in the spatial distribution of activities – inquiry that enables interpretation of territorial disequilibria and hierarchies. Location theory uses the concepts of externalities and agglomeration economies to shed light on such macro-territorial phenomena as disparities in the spatial distribution of activities, thereby laying the territorial bases for dynamic approaches. [1]

[1] CAPELLO, Roberta. *Location, Regional Growth and Local Development Theories, Page 2*

Location theory seeks to explain the distribution of activities in space, the aim being to identify the factors that influence the location of individual activities, the allocation of different portions of territory among different types of production, the dividing of a spatial market among producers, and the functional distribution of activities in space. These various phenomena are analyzed by removing any geographical (physical) feature that might explain the territorial concentration of activities, so that location choices are interpreted by considering only the great economic forces that drive location processes: agglomeration economies, which cause activities to concentrate. [2]

Location theory seeks to explain and define concentration of certain activities in given space in environment of surrounding actors – households, companies, organizations and governments, which suit for our needs in question of security in intangible cyber world. Even though the Cyber Security does not involve any traditional measures as meters and borders, in this explanation it is not relevant as location theory tries to explain differences among regions and states and understand their decision making where computers and other devices serves only as a tool to achieve certain goal. Location theory should give us classical micro and macro economical reasons why actors on global level act in certain way. [3]

1.1.2. Actor-Network Theory

Interaction among actors in the network, describing their relations and influences is reflected in Actor-Network Theory, which became popular in the 1990s, is more frequently applied in geography. In this theory, the social world is presented as a diverse network of relations and influences between different subjects – actors (entrepreneurs, local government) and objects (enterprises, communes, towns, economic regions). [3]

Actor-Network Theory (ANT) is notoriously difficult to summarize, define or explain. There are a number of reasons for this, not least of which is ANT's unrelenting attack on the categories and concepts that have been part of Western thought for centuries.[4]

Coming from the field of Science and Technology Studies (STS), Actor-Network Theory (ANT) is widely known for its disrespectful restatement of concepts central to sociological theory. Its focus on symmetry has challenged commonly held beliefs that human and non-

[2] CAPELLO, Roberta. *Location, Regional Growth and Local Development Theories, Page 3*

[3] SZAJNOWSKA-WYSOCKA, ALICJA. *THEORIES OF REGIONAL AND LOCAL DEVELOPMENT – ABRIDGED REVIEW*

[4] CRESSMAN, Darryl. *Simon Fraser University: A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation*

human agency are different; its insistence on heterogeneity of networks has arraigned common definitions of social networks. In contemporary (international) political sociology,[5] ANT has been applied to the study of states and political action, offering a potential means to see the state simultaneously as both an actor and a network. ANT offers conceptual and empirical innovations regarding problems of (non-)human agency, different modes of ordering practices, and the performativity of politics. Therefore, it also opens up the possibility of finally overcoming essentializing conceptualizations of human nature in the study of political activity, while also making room for a post-humanist conception of political agency. [5]

Definitions and intepretations of Actor-Network Theory differs among authors and have no clear definition past 30 years. Yet it can be for our purposes described as interaction of individuals and organizations in global network seeking for own benefit.

1.1.3. Marxist Theory

Next theory applicable in topic of this diploma thesis is Marxist Theory, describing uneven growth and spatial differentiation, it's root, mechanics and strings controlling actors in time and space.

Another response to the new structural changes in the international economy, especially the persistent underdevelopment of regions in the third world, was the emergence of a Marxist perspective on regional growth and decline. Marxists theories of uneven growth and spatial differentiation place the roots of the uneven development crisis squarely within the nature of the capitalist system. In contrast to theories in the convergence-divergence debate, authors in this literature argue that neither perspective is correct. In fact, as Martin and Sunley (1998) observe in their review of this literature, the Marxist perspective regards regional growth and decline as neither convergent nor divergent but "episodic." In other words, capitalist accumulation proceeds through lumpy progressions, spurred forward by specific crises, which in turn force capitalists to search for new spatial modes of production. [6]

[5] PASSOTH, Jan H. a Nicholas J. ROWLAND. *Acting in International Relations? Political Agency in State Theory and ActorNetworks*

[6] DAWNKINS, Casey J. *Regional Development Theory: Conceptual Foundations, Classic Works, and Recent Developments*

1.2. Cyber Security Theory

Comparing to other theoretical approaches and studies carried in past decades out in political, economical, education and other areas, cyber security as individual field is a very young area which can be dated back to an uprise of internet and wider use in general public thanks to it's accessibility. Since this time can be traced some signs of public and private bodies dealing with security indicent that occurred in cyber world.

„Cyber security", a concept that arrived on the post-Cold War agenda in response to a mixture of technological innovations and changing geopolitical conditions. Cyber security was first used by computer scientists in the early 1990s to underline a series of insecurities related to networked computers, but it moved beyond a mere technical conception of computer security when proponents urged that threats arising from digital technologies could have devastating societal effects Throughout the 1990s these warnings were increasingly validated by prominent American politicians, private corporations and the media who spoke about „electronic Pearl Harbors" and „weapons of mass disruption" thereby conjuring grave threats to the Western world. [7]

The term „cyber security" was widely adopted during the year 2000 with the 'clean-up' of the millennium software bug. When the term „cyber security" is used, it usually extends beyond information security and ICT security. ISO defined cyber security as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace. The Netherlands defined cyber security more broadly, to mean „freedom from danger or damage due to the disruption, breakdown, or misuse of ICT." The danger or damage resulting from disruption, breakdown or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information. [8]

The ITU, United Nations specialized agency for information and communication technologies, also defined cyber security broadly as: „The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include

[7] HANSEN, Lene a Helen NISSENBAUM. *International Studies Quarterly: Digital Disaster, Cyber Security, and the Copenhagen School*

[8] NATO Cooperative Cyber Defense KLIMBURG, Alexander. : National Cyber Security Framework Manual , *Page 12*

connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality." [9]

The internet, the ICT that underpin it and the networks that it connects are at times also referred to as comprising „cyberspace". Merriam-Webster defines „cyber" as: of relating to, or involving computers or computer networks (as the Internet). Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks. The ITU uses the term to describe the 'systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks. The International Organisation for Standardisation (ISO) uses a slightly different term, defining cyber as 'the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form. [10]

Cyber security is branch of information technologies known as information security applied for computers as well as networks. Aim of the information security is safety of information and property from stealing, corruption and natural disasters whereas the information and property must be accessible and productive for presumed user.[11]

By term security of information systems is understood as collective steps and mechanism where sensible and worthy information and services are protected from disclosure, damage or collapse by unauthorized activity from untrusted person or event. Strategies and methods of information security always vary from other information technologies. Our intention is thus to preserve absolute information security against unauthorized persons as well as to preserve functionality and security of end stations thus the network to ensure it's normal working process.

[9,10] NATO Cooperative Cyber Defense KLIMBURG, Alexander. : National Cyber Security Framework Manual , *Page 12*

[10] NATO Cooperative Cyber Defense KLIMBURG, Alexander. : National Cyber Security Framework Manual *Page 8*

[11] *Kybez: Základní názvosloví*

1.2.1. Definition of Cyber Crime

Cyber crime general definition, description of particular points and penalties of commiting a cyber crime differs in time and space across the world. The first attempts to define a cyber crime started in Europe and then followed by other regions on the world.

There does not appear to be a common view regarding what constitutes illegal or illicit activity on the internet. Yet most would agree that one of the fastest-growing areas of crime is that which is taking place in cyberspace. Efforts to clarify and address this issue began in the United Nations (UN) in 1990, where the General Assembly (UN GA) debated and adopted a resolution dealing with computer crime legislation which was later expanded in 2000 and again in 2002 to combat the criminal misuse of ICT. As a result, these early discussions encouraged countries to update their penal codes. For example, in 1997, the Russian government updated the Russian Penal Code (Chapter 28) to address cyber crime, IT crime, and cyber terrorism. Penalties were identified for, among other things, illegal access to the information on a computer, computer systems and networks; creation, spreading and usage of harmful software and malware; violation of operation instructions of a computer, computer systems and networks; illegal circulation of objects of intellectual property; illegal circulation of radio-electronic and special high-tech devices; and manufacturing and spreading of child pornography. [12]

The Council of Europe (CoE) also adopted a Convention on Cybercrime in July 2004,52 the first international convention to address this issue. It contains a relatively high standard of international cooperation for investigating and prosecuting cyber crime. It recognised that criminals exploit the seams of cross-jurisdictional cooperation and coordination among nations. The treaty defined key terms such as ‘computer system’, ‘computer data’, ‘traffic data’, and ‘service provider’ in an effort to create commonality among signatories’ existing statutes, but does not define the key term ‘cybercrime’. [13]

Other world authorities have simultenously defined their own definitions and borders of legal acting on computer which was followed in Asia. Association of South East Asia (ASEAN) has additionally defined a term information war defined as confrontation between two or more states in following words.

[12] NATO Cooperative Cyber Defense KLIMBURG, Alexander. : National Cyber Security Framework Manual , Page 14

[13] NATO Cooperative Cyber Defense KLIMBURG, Alexander. : National Cyber Security Framework Manual , Page 14

Other organisations have taken similar approaches, within their own frameworks. In July 2006, the ASEAN Regional Forum (ARF) issued a statement that its members should implement cyber crime and cyber security laws 'in accordance with their national conditions and should collaborate in addressing criminal and terrorist misuse of the Internet.' These commitments were later codified in the 2009 agreement within the Shanghai Cooperation Organization (ASEANChina Framework Agreement) on information security. Additionally, it is the only international treaty that addresses concerns of a wider concept of 'information war', which the treaty defined as 'confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, and undermining political, economic and social systems, mass brainwashing to destabilise society and state, as well as forcing the state to take decisions in the interest of an opposing party.' [14]

1.2.2. Cyber Security on governmental level

Since the computers started to be used across all sectors making a computer as universal tool for every day's work together with the use of internet, interal networks and public networks as a hub of data transition, concenrs about security challenges emerged on state, public and private sector gradually becoming important on regional and conctinental level due to massive wave of globalization.

Separately, governments are defining what they mean by cyberspace in their national cyber security strategies (NCSS). For example, in its 2009 strategy paper, the United Kingdom refers to cyberspace as 'all forms of networked, digital activities; this includes the content of and actions conducted through digital networks. [14]

By adding the phrase, „the content of and actions conducted through," the government can also address human behaviours that it finds acceptable or objectionable. For some nations, this includes consideration of internet censorship, online information control, freedom of speech and expression, respect for property, protection of individual privacy, and the protection from crime, espionage, terrorism, and warfare. Governments, businesses, and citizens know intuitively that cyberspace is man-made and an ever-expanding environment, and that therefore the definitions are also constantly changing. [14]

Most governments start their NCSS process by describing the importance of 'securing information', implementing 'computer security' or articulating the need for 'information

[14] NATO Cooperative Cyber Defense KLIMBURG, Alexander. : National Cyber Security Framework Manual, Page 8-14

assurance'. These terms are often used interchangeably, and contain common core tenets of protecting and preserving the confidentiality, integrity and availability of information. 'Information security' focuses on data regardless of the form the data may take: electronic, print or other forms. [15]

„Computer security“ usually seeks to ensure the availability and correct operation of a computer system without concern for the information stored or processed by the computer. 'Information assurance' is a superset of information security, and deals with the underlying principles of assessing what information should be protected. Effectively, all three terms are often used interchangeably, even if they address slightly different viewpoints. Most unauthorised actions that impact any of the core tenets or information security attributes36 are considered a crime in most nations. [15]

The implementation, maintenance and improvement of national cyber security comprises a range of elements. These can address strategic documents of political nature, laws, regulations, organisational and administrative measures, such as communication and crisis management procedures within a State, but also purely technical protection measures. Furthermore, awareness raising, training, education, exercises and international cooperation are important features of national cyber security. Thus, the aspects to be considered reach from the strategic through the administrative or operational to the tactical level. [15]

Most governments start their NCSS process by describing the importance of „securing information“, implementing „computer security“ or articulating the need for „information assurance“. These terms are often used interchangeably, and contain common core tenets of protecting and preserving the confidentiality, integrity and availability of information. „Information security“ focuses on data regardless of the form the data may take: electronic, print or other forms. „Computer security“ usually seeks to ensure the availability and correct operation of a computer system without concern for the information stored or processed by the computer. „Information assurance“ is a superset of information security, and deals with the underlying principles of assessing what information should be protected. Effectively, all three terms are often used interchangeably, even if they address slightly different viewpoints. Most unauthorised actions that impact any of the core tenets or information security attributes are considered a crime in most nations. *15*

[15] NATO Cooperative Cyber Defense KLIMBURG, Alexander. : National Cyber Security Framework Manual, Page 1 - 14

The globalisation of the ICT marketplace and increasing reliance upon globally sourced ICT products and services can expose systems and networks to exploitation through counterfeit, malicious or untrustworthy ICT. And while not defined in diplomatic fora, the term „ICT security“ is often used to describe this concern. In general, ICT security is more directly associated with the technical origins of computer security, and is directly related to „information security principles“ including the confidentiality, integrity and availability of information resident on a particular computer system. ICT security, therefore, extends beyond devices that are connected to the internet to include computer systems that are not connected to any internet. At the same time, the use of the term „ICT security“ usually excludes all questions of illegal content, unless they directly damage the system in question, and includes the term „supply chain security“ [16]

1.3. Re-engineering theory

Following theory is addressing to suggestion part which contains roots and signs in restructuring the way of conducting an organization together with application of new tools, frameworks, processes in order to achieve better results.

The idea of re-engineering was first propounded in an article in Harvard Business Review in July–August 1990 by Michael Hammer. The method was popularly referred to as business process re-engineering (BPR), and was based on an examination of the way information technology was affecting business processes. [17]

A first, brief review lead to the conclusion that Business Process Reengineering can be considered as a combined application of theories and and concepts from mainly three areas:

1. Marketing, in the concern of competitive advantage, customer focus, industry value value systems and value adding chains.
2. Organization theory in the broad sense, including the aspects of Human Resource Management and organizational strategies
3. Informatics, the use of IT for supporting process-based organizations by using appropriate information-architectures and -systems. [18]

[16] NATO Cooperative Cyber Defense KLIMBURG, Alexander. : National Cyber Security Framework Manual, Page 9

[17] Business process re-engineering. *The Economist*

[18] SIMON, Kai A*: Towards a theoretical framework for Business Process Reengineering*

The literature on re-engineering employs the term processes. Sometimes it is a synonym for activities. Sometimes it refers to activities or sets of activities that cut across organisational units. In any case, however, the essential notion is the same—both strategic and operational issues are the best understood at the activity level. Business process re-engineering promised a novel approach to corporate change, and was described by its inventors as a "fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical measures of performance such as cost, quality, service and speed". [19]

Furthermore, Hammer considers four keywords within that definition as being the most relevant ones, as there are:

1. Fundamental two questions are considered as being fundamental and are adressing the companies justification of existence: What are we doing? and Why are doing so? As Hammer points out, forcing people to question the way they do business leads to rules turning out to be obsolete, erroneous and inappropriate. Reengineering means starting from scratch, no assumptions given and no current fact accepted and determines firstly what a company has to do, and secondly how to do it.

2. Radical Radical redesign of business processes means getting to the root of things, not improving existing procedures and struggling with suboptimizing. According to Hammer, radical redesign means disregarding all existing structures and procedures and inventing completely new ways of accomplishing work.

3. Dramatic Reengineering is no way for achieving marginal improvements and fine-tuning. It is intended to achieve heavy blasting.

4. Processes Process-orientation is considered as being the most important aspect of BPR. Hammer claims, that most companies are focussed on tasks, people and structures rather than processes. Despite this rather populistic definition, the following paragraphs will provide a more humble definition of the BPR-concept and a brief description of a sample methodology [20]

BPR is generally conceived as consisting of four elements to be considered, as there are strategies, processes, technology and humans (see figure 2.1.), where strategies and processes are building the ground for the enabling utilization of technologies and the redesign of the

[19] Michal Porter, Business process re-engineering. *The Economist*

[20] SIMON, Kai A*: Towards a theoretical framework for Business Process Reengineering*

human activity system. A brief description of these four dimensions will be given below, while a more extensive discussion of the organizational and technological aspects. [21]

Strategies The strategy dimension has to cover strategies within the other areas under concern, namely organization strategy, technology strategy and human resources strategy. The determination of all strategies has to be performed with respect to the dynamic marketplaces the organization is acting on and is not focussed on internalities, but the external presumptions for successful acting on markets. Beyond that, strategies have to be current and relevant to the company's vision, as well as to internal and external constraints, which implies, that a reconsideration and redefinition of strategies might be a presumption for further change. Finally, the strategies must be defined in a way that enables understanding and motivation of employees in order to align the work force with them. [21]

Processes can be defined on different levels within the organization. The issue is, to identify core processes which are statisfying customer needs and add value for them. It is important to point out, that processes are not determined by internal organizational requirements, but by customer requirements, even though organizational constraints have to be taken under consideration. The shift from functional departments to interfunctional processes includes a redesign of the entire organizational structure and the human activity system and implies process- instead of task optimizing. [21]

Information technology is considered as the major enabler for spanning processes over functional and organizational boundaries and supporting process driven organizations. However, the point is not to use IT as an improver for existing activities, as which it often has been conceived, but as enabler for the new organization. This includes using new technologies such as groupware, as well as new methods for using them and an acceptance of technological changes and the fact that information technology will be shaping the future. [21]

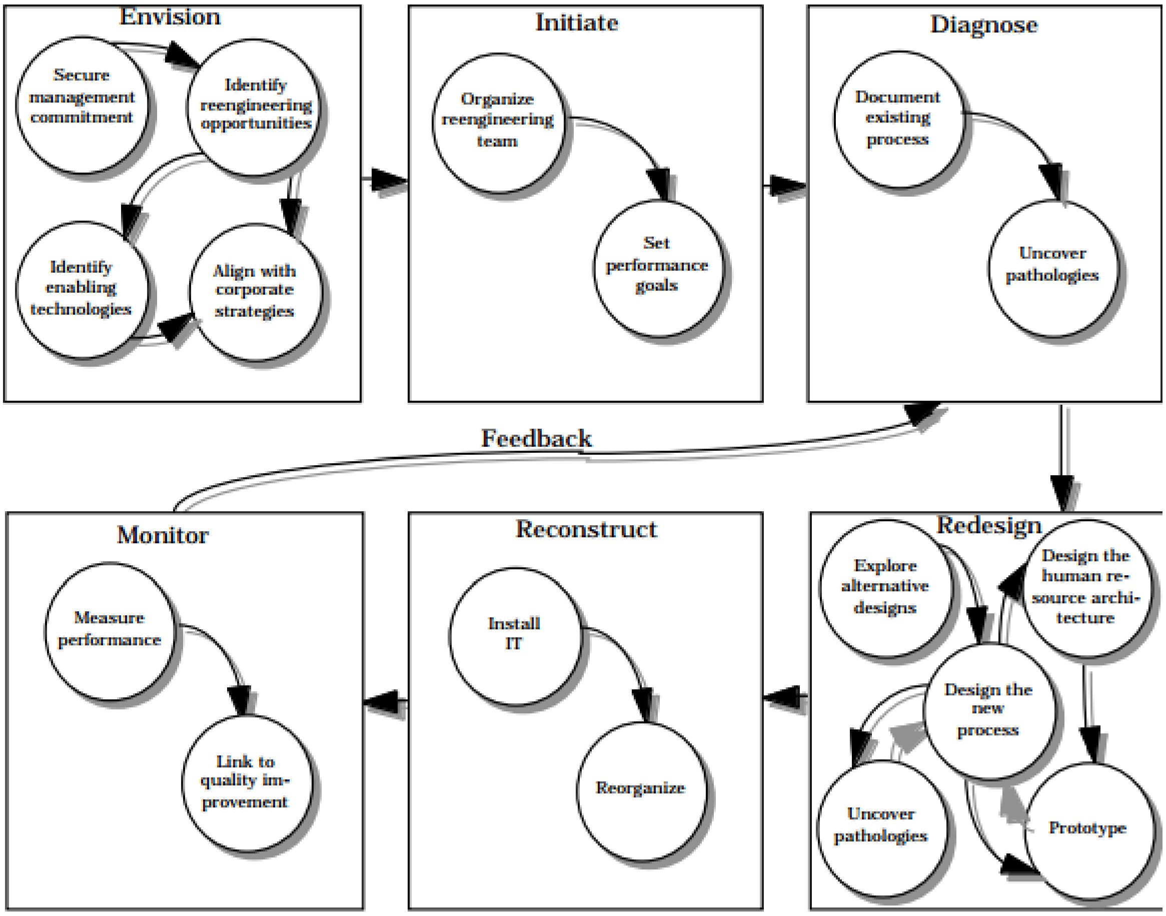
The human activity system within the organization is the most critical factor for reengineering. While top management support for reengineering efforts is rather simple to ensure, the real change agents, middle management are far harder to win due to the fact, that they have to identify change opportunities and perform them, while they are the group facing most threats, as BPR often is used for cutting hierarchies and reducing the work force. The other crucial factor is to align the work force with the strategies defined and to adress the variable cultural and environmental contexts within the organization. Finally, flattening

[21] SIMON, Kai A*: Towards a theoretical framework for Business Process Reengineering*

hierarchies implies decision making to be moved down in the organization and empowerment of the employees taking them. This requires training and education as well as motivation and trust from top management that people are able and willing to take responsibility, a fact that is rather contradictory to the "trust is good, control is better" way of thinking. [22]

As this concept has focused on application of IT technologies which were innovative to implement in business processes, IT divison of security experience in recent years a similar situation, calling for implementation of same methods as in Business Process Re-engineering theory. Such process is described and depicted on following figure.

Graph 1: Re-engineering methodology approach


Envision
Secure management commitment
Identify reengineering opportunities
Identify enabling technologies
Align with corporate strategies
Initiate
Organize reengineering team
Set performance goals
Diagnose
Document existing process
Uncover pathologies
Feedback
Monitor
Measure performance
Link to quality im-provement
Reconstruct
Install IT
Reorganize
Redesign
Explore alternative designs
Design the human re-source archi-tecture
Design the new process
Uncover pathologies
Prototype

Source: Kai A. Simon, Towards a theoretical framework for Business Process Re-engineering

Theoretical part have included all relevant theories that can be applied in certain way in topic of diploma thesis dealing with increasing level of cyber security for blossoming regional development of the region.

[22] SIMON, Kai A*: Towards a theoretical framework for Business Process Reengineering*

2. Analytical part

In the practical section, I would like to begin with legal aspects and formal bodies that have adressed the question of cyber security and personal data protection firstly in draft which have later on turned into official convention that should represent a strategies and frameworks for member states of African Union dealing with cyber security issues. In connection with cyber security and official document called African Union convention on cyber security and personal data protection adopted on 27th June 2014, will be collected and summarized official guidelines, requierements, threats and gaps that were concluded and considered as relevant areas by member of African Union.

After deeper study of the convention and areas that are connected with the subject of my diploma thesis I will stress out actual facts and figures that encourage the importance of information security in current environment of second decade in 21st century with threats, costs, trends and opportunities that are emphasizing the need of data security.

The question of data security requires also the need to control, organize and manage organization's assets from information, information technology sources to human capital which is another area of the analytical part of my thesis. Those three sources all together represent three actors that are subject of the African Union's convention. It's necessary to realize that actors named above are subjects that occur and operate in cyber space even though they are not specified in the convention, but they are the actors that together create cyber space. The question of effective management of organization resources is not explicitely mentioned problem and area to solve in the convention, however it is directly connected with dilemma of the information security and always uses and requires similar tools. Why would such tools to control and manage over organization assets contribute to security in general is underlined by one rule „What you do not know about, you do not control.".

Next argument for control over assets in organization relies in the question of information and organization's security that was in 20th and earlier 21st century focused on external threats, however, this attitude has to also focus on users and internal oriented questions since the threats could be also hidden inside. Concept of information security concern then not only tools to, for example, encrypt files but also to control where the information moves, what user have edited etc. Such methods however reveal also other aspects that can be gathered from the information and such aspects have economical character, where managers can easily see and control what is in accordance with employee's work and what is personal, inefficient or harmful usage. For those reasons were also included question of efficient usage of organizations assets as a relevant topic to deal with.

Analytical part is divided into two logical parts where first one covers the analysis and comments on African Union Convention as legal basis and justification of Cyber Security Concept. Case studies described in second part describes current trends in cyber security, typical targets and sources of such attacks, motivations behind attacks, average calculation of such security incidents and an estimation of implementing security measures.

2.1. Analysis of African Union Convention

It is important to keep in mind that initial incentives in use of modern technologies and tools in monitoring and analyzing work on computers has its roots in security issues and is the main driver up till today. African Union and European Union are typical examples where cyber space is perceived as extremely important and very dangerous source of information thus it represents a huge potential threat. It's growing importance also relies on the fact that cyber space does not respect all physical dimensions like distance and borders. Thus every single internal site is exposed to every single human acting in cyber space. Relevant argument why had this trend accelerated such significantly in the 20th and 21st century is the increase in number of cyber attackers. They have become far more sophisticated thanks to publicly accessible technologies and the level of knowledge to be able to commit a crime have fallen somewhere to highschool age, making it easier for anyone to attack as a single person on internal sites of companies that are countlessly bigger.

African Union introduced in October 2012 draft on convention about cyber security and confidence which suggest to set up basic rules and obligations that propose adopation on the level of African Union, providing credible framework in cybersecurity in Africa through organizations with electronic transactions, protection of personal data, e-governance, promoting cyber security and combating cybercrime. Those conditions mentioned in the proposal includes also as a relevant subject governments of African Union.

According to African Union Draft, the transnational nature of cybercrime calls for a focused attention on its multiple dimensions: scientific, technological, economic and financial, political and socio-cultural. The interaction of these dimensions reinforces the complexity of cyber security that manifests at several levels:

- Informational security impacts on the security of the digital and cultural heritage of individuals, organizations and nations
- The vulnerability in the normal functioning of institutions can compromise the survival and sovereignty of States [23]

Relevant dimensions in the draft directly related with information technologies need to preserve their security, integrity and functionality resulted in following challenges for member states of African Union:

- Achieve a level of technological security adequate enough to prevent and effectively control technological and informational risks
- Build an information society that respects values, protects rights and freedoms, and guarantees the security of the property of persons, organizations and nations [23]

Several elements on the conceptual level that relates with the topic of diploma thesis were also mentioned as a neccessary points to create a climate of confidence such as:

- Predictable in terms of prevention and resolution of disputes; and evolving because it takes into account the continued technological evolution
- Organized: covering the relevant sectors
- Protective: of consumers and intellectual property (civil and penal) of citizens, organizations and nations
- Secured: striking proper balance between legal and technological security [23]

Two years later in the official convention of African Union adopted on 27th June 2014 stakes and challenges discussed in the draft have not changed much and they have got more detailed structure and specific points that together create a complex framework to follow. According to the convention on Cyber Security and Personal Data Protecion (CSaPDP) Member States of the AU considers that this Convention on the Establishment of a Legal Framework for Cyber-security and Personal Data Protection embodies the existing commitments of African Union Member States at sub-regional, regional and international levels to build the Information Society. [24]

[23] DRAFT AFRICAN UNION CONVENTION ON THE CONFIDENCE AND SECURITY IN CYBERSPACE. *NATO Cooperative Cyber Defence Centre of Excellence*
[24] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

The quesiton of law and humar right corectness is also reflected in the concept of Cyber Security and Personal Data Protection. Member states consider also that the establishment of a regulatory framework on cyber-security and personal data protection takes into account the requirements of respect for the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human rights Conventions and Treaties, particularly the African Charter on Human and Peoples' Rights. [25]

It is beared on mind that the major obstacles to the development of electronic commerce in Africa are linked to security issues, particularly to the question of (i) The gaps affecting the regulation of legal recognition of data communications and electronic signature (ii) The absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems (iii) The application of electronic techniques to commercial and administrative acts (iv) The probative elements introduced by digital techniques (time stamping, certification, etc. (v) The rules applicable to cryptology devices and services [25]

Member states of African Union are convinced that the afore-listed observations justify the call for the establishment of an appropriate normative framework consistent within the African legal, cultural, economic and social environment. Therefore the objective of this Convention is to provide the necessary security and legal framework for the emergence of the knowledge economy in Africa. To ensure security and legal framework in African Union will greatly encourage the growth in the regional level thanks to the legislative background for law breaches in cyber world and support in control over the infromation assets and appropriate management of human and IT resources.

Local authorities are concious about importance of cyber security promotion. This need appears also in the Premable of the Convention and calls for involvement of public and private actors in the need and struggle to implement and assure the basic security standards on government level, private sector, civil organization, the media, training and research institutions. These paragraphs from Premable of the Convetion also serve as justification for the target picked up in my diploma thesis together with importance to assess the question of costs, obstacles, threats and other relevant topics that rely in the question of cyber security.

All points mentioned above are relevant to the topic of diploma thesis that wants to appoint on such problems and propose a security draft that could serve as a guide for changes in legal and

[25] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

functional framework on the first level followed by next steps that will be covered in the suggestion part.

Before proceeded further to case studies that show present problems and challenges in cyber security, particular chapters will be analyzed with their limitations and current needs, of the Convetion relates with the question of information security in cyber world. This step is neccessary to analyze in order to be able to propose a draft suitable into African Union environment and needs. Areas related with topic of this diploma thesis includes Personal Data protection, Information Security and Cyber Security.

2.2. Analysis of Legal Aspects – Information Security

2.2.1. Basic concept and understanding of Information Security

Personal Data Protection is actual topic nowdays due to the fact that our sensitive information of bank account, insurance, medical record and health disabilities, information on social networks, agreements and contracts between persons and authorities etc. are all listed, kept and available on closed or even open networks. Objective of the Convetion with respect to personal data ask for commitment of each state party to establish a legal framework aimed on the protection of physical data and punish any violation of privacy to strengthen basic fundamental rights and public freedoms. The established mechanism should ensure that any form of data processing respects the fundamental rights and freedoms of a person while recognizing the prerogatives of the State and the purpose for which the organizations were established.

In the Chapter II. Personal Data Protection Article IX. Describes the scope of application of the convention on following actions:

a) Any collection, processing, transmission, storage or use of personal data by a natural person, the State, local communities, and public or private corporate bodies

b) Any automated or non-automated processing of data contained in or meant to be part of a file, with the exception of the processing defined in Article 9.2 of this Convention

c) Any processing of data undertaken in the territory of a State Party of the African Union

d) Any processing of data relating to public security, defence, research, criminal prosecution or State security, subject to the exceptions defined by specific provisions of other extant laws. [25]

This diversification in actions and limitations in applicability clearly set out the activities and operations that should be standardized and followed by the rules outlined in this convention. In other words it is limited by the borders of the African Union in geographical terms and by basic diversification of personal data by subject that operates with personal data on government, public and private level to comply with fundamental rights and freedoms of citizens. Other data processing related to sensitive data described in the last paragraph above ask for specific provisions for each area respectively.

Following Chapter X. defines the preliminary processing steps of personal data diving them into the most common categories which are not likely to constitute a breach of privacy and individual freedoms and the rest, where protection authority may establish and publish standards to simplify the process or introduce exemptions from the obligation to make a declaration.

With regard to personal data processing undertaken on behalf of the Government, a public institution, a local community, a private corporate body operating in public service, processes should be undertaken with accordance to legislative or regulatory act enacted after an informed advice of the protection authority. Such data processing is related to:

a) State security, defence or public security

b) Prevention, investigation, detection or prosecution of criminal offences, or execution of criminal convictions or security measures

c) Population survey

d) Personal data directly or indirectly revealing racial, ethnic or regional origin, affiliation, political, philosophical or religious beliefs or trade union membership of persons, or data concerning health or sex life. [26]

2.2.2. Definition of Protection Authority

The convetion on Cyber Security and Personal Data Protection also suggests to Each Member State to establish an authority that will be in charge of protecting personal data. In the convention it is reffered as National Personal Data Protection Authority. This Protection Authority should be an independent administrative authority with a task to ensure correct

[26] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

conduction of processing of personal data in accordance with the provisions of this Convention.

The reason for the separate authority dealing with protection issues further described in the Article XI. is to bring out independent suggestions to other authorities the best possible security solutions suitable into their functional framework regardless their own insights. By such authority division you will achieve the best possible outcome from authority's particular field, in this case information protection, and avoid any discrepancies and disputes about one's work. To quote directly two paragraphs from the African Union Convention, the content is as follows:

The national protection authority shall be an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with the provisions of this Convention. Membership of the national protection authority shall be incompatible with membership of Government, carrying out the functions of business executive and ownership of shares in businesses in the information and communication technologies sector. [27]

2.2.3. Duties and Powers of Protection Authorities

The national protection authority should inform responsible persons and processing officials about their obligations. Their will and security proposal to other authorities should not be influenced by any other instruction from different authority in the interest of performace of their duties. Protection authorities should also get full support from state parties covering human, technical and financial resources necessary to accomplish their mission. Such suitable work environment shall ensure the best possible outcomes regardless its costs with reasonable limitations stated by the given member state.

National protection authorities decide and watch over authorities and actors that are mentioned in the African Union Convention to obey of rules, limits and standards in terms of personal data processing. In case of any breaches they are allowed to act as following:

a) Issuance of warning to any data controller that fails to comply with the obligations resulting from this Convention

b) An official warning letter to stop such breaches within a timeframe set by the authority. [27]

[27] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

If the subject is not taking into account those warnings and informative cautions and fails to comply with them, the National Protection Authority may impose following sanction after adversary proceedings:

a) Temporary withdrawal of the authorization granted

b) Permanent withdrawal of the authorization

c) Monetary fine [28]

In extreme cases of breaches of law in terms of violation of fundamental rights and freedoms in processing or use of personal data the National Protection Authority may after adversary proceedings decide as follows:

d) Discontinuation of data processing

e) Blocking of some of the personal data processed

f) Temporary or permanent prohibition of any processing at variance with the provisions of this Convention [28]

2.2.4. Basic principles of personal data processing

Couple of Principles in Chapter of Personal Data protection are dedicated to crucial part of processing, handling and storing of personal data, defining some basic guidance how to treat such information, what is reasonable to collect and legally correct in personal data processing. In cases of allineaton of sensitive personal data that might be harmful to a citizen must be applied adequate security measures to avoid such actions done by third side. Third principle in the chapter related to basic principles of personal data processing describes the limits of the data content based on the purpose and correct processing and storage of such data in following points:

a) Data collection shall be undertaken for specific, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes

b) Data collection shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processes

c) Data shall be kept for no longer than is necessary for the purposes for which the data were collected or further processed

[28] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

d) Beyond the required period, data may be stored only for the specific needs of data processing undertaken for historical, statistical or research purposes under the law. [29]

Such measures should ensure that collected data about citizens obtain only necessary information and are stored and handled in the way to avoid any possible loss of the data. in case of alienation to reduce the readable content of the information for any harmful use. Question of confidential information and security of personal data is described in Principle 6 in following points:

a) Personal data shall be processed confidentially and protected, in particular where the processing involves transmission of the data over a network

b) Where processing is undertaken on behalf of a controller, the latter shall choose a processor providing sufficient guarantees. It is incumbent on the controller and processor to ensure compliance with the security measures defined in this Convention. *29*

Such basic layout of measures should ensure the security of personal data between two subjects and always take into account subject's security and citizens background in order to avoid breaches with law. Member States should undertake to prohibit any data that includes citizen's affiliation in religion, politics, philosophical beliefs and personal information revealing ethnic origin. Information should also not include economical background of the citizen and data containing state of health of the subject. Such information in hand of unauthorized person might have harmful impact on citizens that is inconsistent with basic freedom principles. Such prevention should lead to minimaze the potential negative impact from economical and personal point of view on the person and the data processor, who is in charge for data alienation. The provisions of this Convention shall also include the application of the national legislation to the print media ort he audio-visual sector.

Prohibitions set forth in previous article shall not apply on specific situations. First example is where a citizen has manifestly made the data publicly accessible which is not in power and interest of Member State to regulate. Next group of exception is when judicial procedure or criminal investigation is instituted. Another group relates to situations where is necessary for the performace of a task carried out in the public interest or in the excercise of official authority or assigned by a public authority vested in the controller or a third party. Those exceptions and other related cases listed in the Chapter XIV can handle with the personal data

[29] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

of citizens. Last two points, security and storage obligations, connected with our topic will conclude the part of Information Security, where is described all necessary action of the Member State to take all appropriate precautions according to the nature of the data to prevent such data from being altered, destroyed or unauthorized for third parties. To encourage the citizen's security, the data shall not be kept for no longer than is necessary to avoid any possible complications.

2.3. Analysis of Legas Aspects – Cyber Security

2.3.1. Basic legal background and suggestions in Cyber Security

In this chapter will be analyzed legal aspects of African Union Convention regarding to information security, control over information flow, control and management of IT assets. Those four groups represent initial steps to fight successfully Cyber Crime, where this term doesn not cover only external threats but can be also the question of internal policy and framework dedicated with work with organizations' assets, either tangible or intangible.

The question of promotion of cyber security and dealing with cybercrime might seem at the first glance as a completely different subject from the first analyzed legal aspect of African Union Convention. After close examinations of normally processed data with information in electronic form, it is obvious that legal aspects of Personal Data Protection talks generaly about all data containing citizens' information in different forms – paper either electronic, where as Chapter III about Cyber Security Promotion deals besides fighting cyber crime particularly with IT mediums containing sensitive information and defines a basic rules and standards to follow.

Basic and general advices suggest that every single Member State should develop with collaboration of stakeholders a National Cyber Security Policy where is recognized Critical Information Infrastructure (CII) for the nation and identifies the risks facing the nation using all possible harmful scenarios and outlines how the objectives of such policy are to be achieved. In other words the aim is to identify Critical Information Infrastructure that might have any negative impact in case of loss of data or non-functionality of information systems deemed as sensitive for their National Security and well-being of the economy. National Policy should in this regard also propose more sever sanctions for criminal activities on such Information Systems in these sectors together with identifying security gaps by improving of vigilance, security and management. The question of identification of critical information, their security and crisis management has dedicated part in suggestions called Risk Analysis.

Strategy to implement such policy may differ among Member States and is written as follows: State Parties shall adopt the strategies they deem appropriate and adequate to implement the national cyber security policy, particularly in the area of legislative reform and development, sensitization and capacity building, public-private partnership, and international cooperation, among other things. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cyber security policy and lay the foundation for effective management of cyber security incidents and international cooperation. [30]

Such strategy outlines only areas to target and work on in sectors mentioned above. The strategy should include also organizational structure, defining objectives and responsibilities to implement such policy with basics of management of cyber security incidents and international cooperation, providing only basic framework to focus on. The question of the strategy how to promote better management of cyber security incidents together with organizational structure is partly outcome of the Risk analysis together with Directive of work in ICT defining users and administrator's responsibilities.

Adoption of any legal measures in the area of cyber security and establishing the framework for implementation should be done by each Member State in accordance to the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly human rights from African Charter. Other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others are as well taken into account.

National Regulatory Authority shall be established as in case of Personal Data Protection, defining own limits, standars and rules to control. More accurate form is described in the Convention as follows: Each State Party shall adopt such legislative and/or regulatory measures as it deems necessary to confer specific responsibility on institutions, either newly established or pre-existing, as well as on the designated officials of the said institutions. Conferred statutory authority and legal capacity shall act in all aspects of cyber security application, including but not limited to response to cyber security incidents, and coordination and cooperation in the field of restorative justice, forensic investigations, prosecution, etc. [30]

2.3.2. Role of Government – National Cyber Security System

Role of a government in terms of Cyber Security is to provide enough resources in financial and human capital for development of the cyber security culture within its borders. The

[30] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

support of Cyber Security Authority should be exclusive with aim to promote development in their particular field regardless the needs of other authorities in order to reach and be compatible with standards mentioned in African Union Convention. Member states also undertake to disseminate newly gained information and knowledge from field of cyber security to the public. Each Member State should establish public-private partnership to engange other public, private and academic institutions in the promotion and encouragement of cyber security culture.

Education and training is the key point to ensure the up-to-date cyber security measures within their borders. Each Member State should undertake to develop capacity building with a view to provide traning which covers various areas of cyber security to different stakeholders together with setting standards for the private sector.

State Parties undertake to promote technical education for information and communication technology professionals, within and outside government bodies, through certification and standardization of training; categorization of professional qualifications as well as development and needs-based distribution of educational material. [31]

Continual support and promotion of training, seting up standards to meet and qualifications to specialize on shall ensure basic for continuously developing employees and specialists in particular field.

2.3.3. Cyber Security – Monitoring Structures

Cyber security governance is a term that defines an ability of the organization to monitor, collect, analyze, evaluate and predominantly control over the organization assets. Last point about control is decisive for eliminating the number of information exposed in the network in unsecured perimeter, which is not only a matter of software tools but organization’s framework policy. Adequate tools for tracing the incidents are necessary for improving a current level of cyber security for the future. The Article 27. in its first point generaly describes this need as necessary measures to establish an appropriate mechanism responsible for cyber security governance. Such formulation leaves out necessary point mentioned above and gives an Each Member State on their own responsibility to tackle this area that they deem as critical.

[31] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

Previous paragraph is generaly described in institutional framework of cyber security in following formulation: Each State Party shall adopt such measures as it deems necessary in order to establish appropriate institutions to combat cyber-crime, ensure monitoring and a response to incidents and alerts, national and cross-border coordination of cyber security problems, as well as global cooperation. [32]

In order to achieve the best possible results, private sector and the knowledge with experiences should not be excluded in the national strategy of the Member States. Government sector encourages the private sector to participate in government-led activities to promote cyber security.

Cyber security governance should be established within a national framework that can respond to the perceived challenges and to all issues relating to information security at national level in as many areas of cyber security as possible. [32]

Regarding to broader description and seting up standards with basic guidance, African Union Convention does not provide any further solid basis in this matter. A proposal of various monitoring activities is included in the suggestion part to provide another relevant source based on experiences gathered and analyzed from another countries and environments to elaborate a broader concept covering more aspects promoting cyber security on governmental level.

2.3.4. Cyber Security – Criminal provisions

Whereas previous part about suggestions and standards in African Union Convention was very concise and general for basic common principles and structure of monitoring activities, the Criminal provisions for commiting a crime against a law in terms of cyber world has very broad coverage, divided to more specific areas: Attacks on Computer Systems, Computerized Data Breaches and Information and Communication Technologies covered in the article 29 and 30. Defining a concrete examples of law violations in each category will bring Member States a document which facilitate the criminal judiciary procceses defining what kind of crime was committed to avoid any wrong assessments of law breaches in terms of cyber crime.

[32] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

In the context of Attacks on Computer systems the Convention suggests to take the necessary legislative and/or regulatory measures to make it a criminical offence in case of following situations:

a) Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access

b) Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access with intent to commit another offence or facilitate the commission of such an offence

c) Remain or attempt to remain fraudulently in part or all of a computer system

d) Hinder, distort or attempt to hinder or distort the functioning of a computer system

e) Enter or attempt to enter data fraudulently in a computer system

f) Damage or attempt to damage, delete or attempt to delete, deteriorate or attempt to deteriorate, alter or attempt to alter, change or attempt to change computer data fraudulently. [33]

In the first three points are generally defined offenses against law gaining unauthorized access. Worth mentioning remark is that this broad definition covers from external citizens trying to get an access to employees that would exceed their authorized access and permission with harmful intention against the given person or organization. Other points include attempts to negatively affect fluent functioning of the system and handling the data stored in the computer systems in negative way to harm a person or organization. Further description of fraudental and criminal use of data is described in the next point of Article XXIX in following points:

a) Intercept or attempt to intercept computerized data fraudulently by technical means during non-public transmission to, from or within a computer system

b) Intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches

[33] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

c) Knowingly use data obtained fraudulently from a computer systém

d) Fraudulently procure, for oneself or for another person, any benefit by inputting, altering, deleting or suppressing computerized data or any other form of interference with the functioning of a computer system

e) Even through negligence, process or have personal data processed without complying with the preliminary formalities for the processing [34]

Legislative and regulatory measures to criminal offences in data alienation and unauthorized use with intent to harm the subject with clash with legislation should ensure an appropriate judicial procedure corresponding to seriousness of the crime commited. Such legislative measures should preserve citizen's security and in case of any fraudulental procure of their identity the person responsible for commiting the crime will be adequately prosecuted. The Convention focuses to combat particularly organized crime commited by organizations where sanctions for any law breaches under the aegis of criminal organization will be punishable by the maximum penalty prebscribed for the offense.

2.4. Analysis of implemented legal framework of South Africa

South Africa as one of the first states in African Union was the first to implement The National Cybersecurity Policy Framework in March 2012 which have been that time a step forward which was in certain way innovative in global measures. South Africa was ahead to regional states of African Union being a good example of managing newly upcoming risks in cyberspace territory. In their own National Cybersecurity framework were identified and closely defined terms such as: Cyber Security, Cyber Space, Cyber Warfare, Cyber Espionage, Cyber Terrorism, Cyber Crime, Organization and user's assets and other showing an awareness of up to date problems.

One of the points mentioned covered in the African Union Convention as well as in South Africa's National Policy Framework was delegating a separate authorities dealing with cyber security problems that was named foreseen to establish centralized structure in order to address, anticipate cyber threats and response to them. This initiative resulted in establishement of three separate bodies: National Cyber Security Coordinating Centre (NCSC), National Critical Information Infrastructure Protection (CII) and Computer Security Incident Response Team (CSIRT). The objective of those separate authorities was obvious.

[34] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION*

To address recent threats, forecast their development, form a post-incident framework to recove without the least possible losses in the shortest time and to disseminate cyber security culture among state, private and public organizations together with general public.

This framework is intended to implement an all encompassing approach pertaining to all the role players (state, public, private sector, civil society and special interest groups) in relation o Cybersecurity. This framework will be supported by a National Cybersecurity Implementation Plan which will be developer in consultation with relevant stakeholders, indentifying rols and responsibilities, timeframes, specific performance indicators and monitoring and evaluation mechanisms. The development and large-scale implementation of a system of security measures as implemented elsewhere in the world will form part of the National Cybersecurity Implementation Plan. [35]

The National Cybersecurity Policy Framework recognises that the State is charged with implementing a government led, coherent and integrated cybersecurity approach which, amongst others, will:

a. Promote a cybersecurity culture and demand compliance with minimum security standards

b. Strenghten intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and adressing cybercrime, cyber terrorism and cyber warfare

c. Establish public-private partnerships for national and international action plans

d. Ensure the protection of national critical information infrastructure

e. Promote and ensure a comprehensive legal framework governing cyberspace. [35]

All above mentioned points corresponds with the Convention that have been in those particular points more descriptive and accurate. To address some of the chapters, in the Convention were determined criminal provisions for commiting cyber crimes making universal suggestions how and for what crimes should be treated accused persons.

Compared to proposals of African Union Convention, South Africa was already ahead in establishing authorities in dealing in this new, undiscovered territory with new challenges. One of particularly important topic was covered in South Africa’s plan as well, calling for need of cryptographic devices or softwares, that ensure secrecy of information. National

[35] National Cybersecurity Policy Framework for South Africa. *Cyanre South Africa*

Cybersecurity Policy Framework noticed that several attempts on regulating cryptography were initiated in different documents, strategies and laws that goes as follows:

- National Convention Arms Control Act (Act 41 of 2002)
- Electronical Communications and Transactions Act (Act 25 of 2002
- Electronical Communications Security (Pty) Ltd Act (Act 68 of 2002)
- Regulation of Interception of Communications and Provision of Communications Related information Act (Act 70 of 2002)
- State Information Technology Agency Act (Act 88 of 1998)
- Conventional Arms Control Regulations (R7969 of 2004)

f. Cryptographic regulations (R8418 of 2006) [36]

None of above mentioned laws however reflect up to date security issues, framework of processes, new coming information that started to be used and stored in cybersphere which asks for cryptography tools and other factors, leaving these documents outdated and not reflecting current needs and gaps. All documents have been recommended to revise and develop a new integrated framework for cryptography to address new challenges.

South African authorities have taken an advantage of already implemented National Policies on Cybersecurity of different nations, namely Australian, Japan, Malaysian, United Kingdom, Germany and other organizations, which outlined a good basis for creation of their own framework with implication of local problems. By such knowledge and information collection they have made a very solid milestone to build on in area of cyber security. Despite a good and solid legal basis in South Africa there are still increasing number of incidents that have negative impact on regional development of the region.

2.5. Case studies related to Cyber Security

Where as first parts of the Analytical part showed the conciousness of African Union Members through the Convetion to express the importance and need to harmonize the legislative environment in the area of cyber security, the aim of upcoming part is to analyze the current trends in cyber security, growing number of incidents and demonstrate the comparison of total costs of commited cyber crime in last years, it's minimum, average and

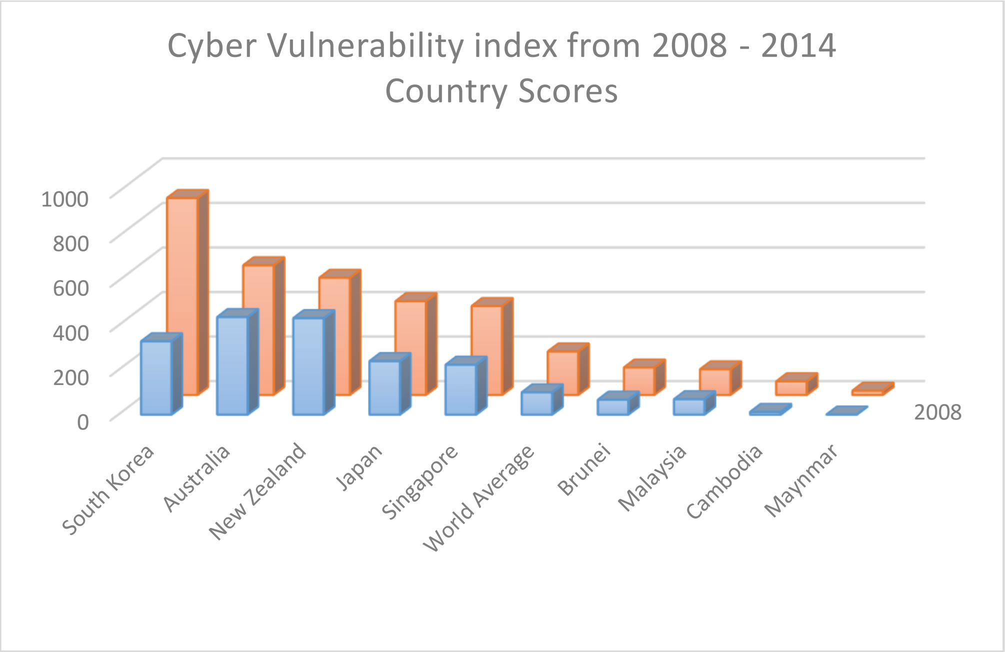
[36] National Cybersecurity Policy Framework for South Africa. *Cyanre South Africa*

extreme situations. Combination of these two backgrounds in form of initiative and support on governmental level to combat cyber crime, cyber security and control over information together with case studies summarized in following chapters should serve as an adequate justification to take action in core sectors of the government and related institutions to be in accordance with legal and regulatory standards stated in this convetion. Following case studies from different sources should allocate all important and concise information pointing on growings seriousness in past years.

2.5.1. Cyber Vulnerability Index

Basic indicator showing on most endangered regions and states in given time. The vulnerability in terms of cyber attacks and incidents relies on more factors at once. Worldwide consultancy firm Delloite described the vulnerability to cyber attacks based on how extensive a economy relies on Internet-based interactions. Cyber Vulnerability Index was compiled by Delloite company based on historical data from the World Bank's World Developement Indicator using each nation's rate of mobile cell subscribers, number of secure Internet servers, fixed broadband subscribers and rate of Internet use. It is important to keep in mind that particularly this index have progressively rising number changing every year in higher numbers resulting in negative results in terms of cyber security. Following data were collected and measured in Asian Region, difference in past 8 years period showing a flourishing player in terms of internet users with booming economies in few aglomerations.

Graph 2: Cyber Vulnerability Index in Asia from 2008 - 2014



Source: Channel NewAsia, Vulnerability to Cyber attacks 2016, edited by author

The data collected from World Bank and processed by Delloite company shows up the growing trend for every assessed subject ranging from double to almost triple increased value. The index reflects basically the number of users, internet connections and wireless connections on various devices which directly negatively influence the growing value of this index, resulting in more vulnerable subjects in cyber space.

To imagine the situation in case of African continent, more revealing statistics covering variables of Cyber Vulnerability Index that were allocated by Bloomberg in World Data Protection Report from May 2015, which addresses significant increase in the users and issue of data leakage to terrorist organization. According to a serving foreign intelligence officer recently interviewed by The Guardian, the continent of Africa has become the El Dorado of espionage. The statement folowed a leak of South African security files to Al Jazeera revealing the extent of spying aktivity within its borders. [37]

The presence of spying agents was determined for economic and technological theft amont the principal reasons. Reasons of espionage can be easily traced to it's main donors. Trillions of dollars were recently invested in recent years which has given foreign powers greated influence in Africa, but not all activities has been overt and transparent. The Al Jazeera sources allege that China broke into South Africa's main atomic research facility in attempt to steal information on the country's pebble bed nuclear reactor. [37]

In other examples of national espionage can be observed revealing cases of nation espionage done on corporations to advance their positions and interests in worldwide field.

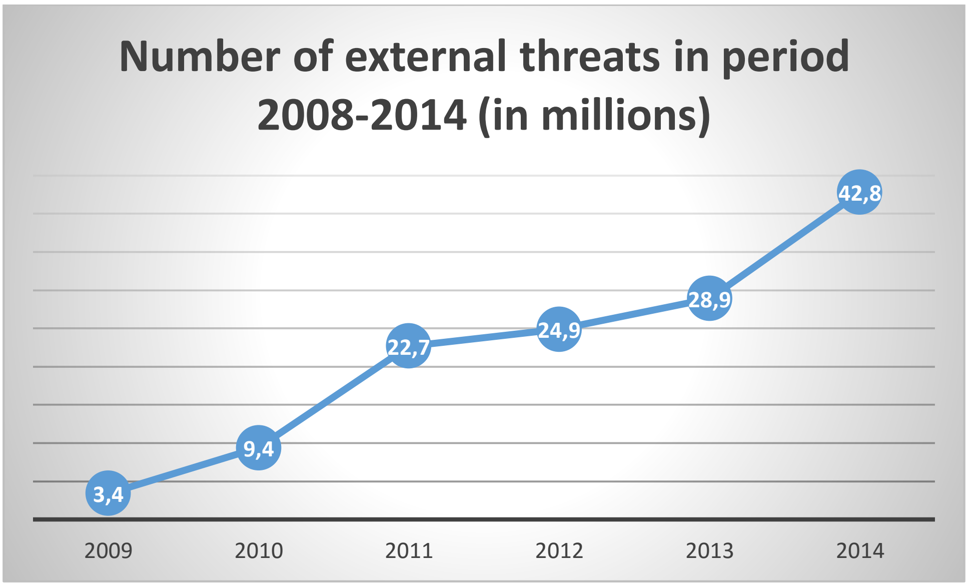
The investments have brought to recepient's continets besides the uncertain questions of espionage obvious and observable outcomes. The question „Why are cyber attacks a growing threat in Africa?" can be answered by investments into Africa, particularly to infrastructure to build up communication networks, integrate interner, provide an access of cell phones in general public. Cisco predicted that there will be about 600 million smart devies in Africa by 2018, up from 133 million two years ago together with cloud storage traffic expected to increase by over 800 percent between 2012 and 2017. Those facts and at the same time variables of Cyber Vulnerable index points on increasing threat of potential cyber attacks in the future.

[37] MULLIGAN, Helen a Owen O'RORKE. *Bloomberg: World Data Protection Report*, The Growing Threat of Cyber Attacks in Africa

2.5.2. Number of security incidents

With investement coming into technical infrastructure in developing countries comes besides the technical uprise in general public also the negative wave of treaths beneath. According to the Global State of Information Security Survey the total number of external threats is growing by 117 339 incoming attacks every day, where the total number of security incidents detected and registered by respondents climbed to almost 43 millions for 2014, 48% increase over the year 2013. Trend of the external attacks in past 5 years is showed in following graph.

Graph 3 : Growing number of external threats from 2009 to 2014



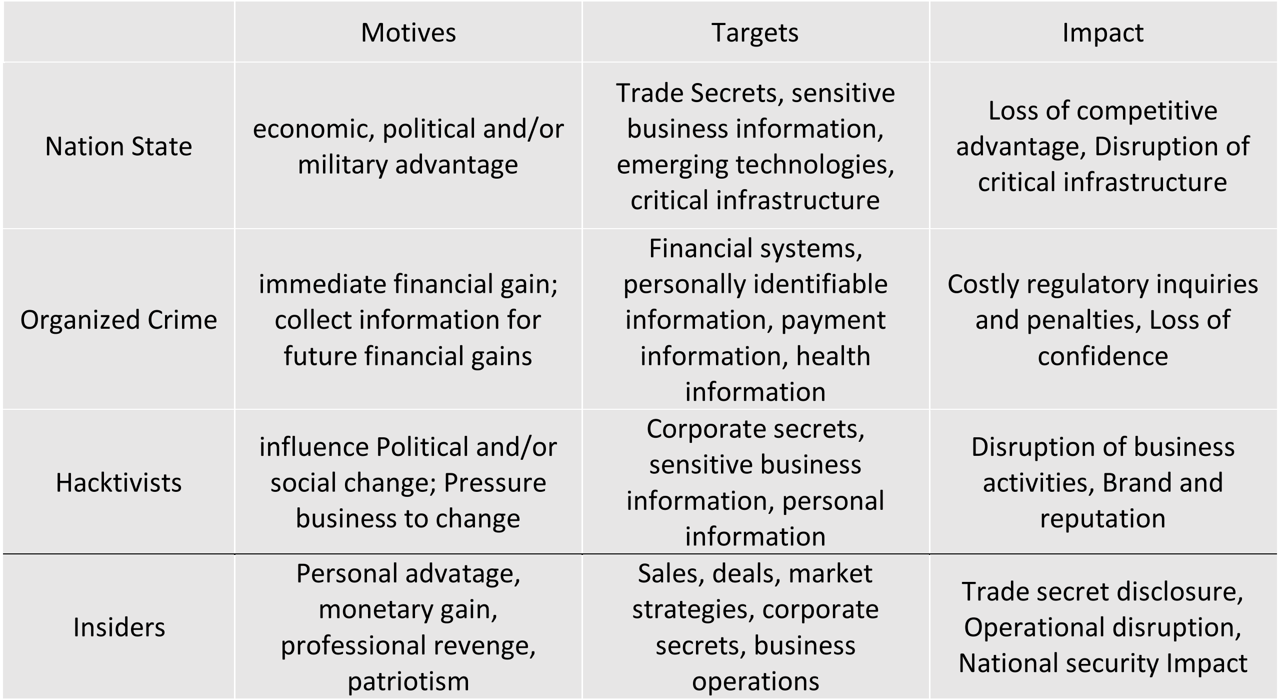
Source: Global State Information Security Survey 2015, PwC, edited by author

Increasing number of external threats wasn't valid only for years 2013 and 2014, but the most significant difference can be observed in preceeding years, particularly between 2010 and 2011. In absolute numbers the gap in 5 years accounts 40 million external threats difference observed and noted by the questioned subject. The real number might be even higher however there is lack of evidence for those attacks or attempts that were not registered by the subjects. Trend and different intentions behind such external attack will be further described in the following chapter dedicated to type of attacks. The information about total number of attacks differs based on the nature and type of the attack and nature of the attack making it difficult to find a adequat and compact information from trustworthy sources.

2.5.3. Typical target and type of attacks

General intention of the attacks against a subject can have various reasons behind, ranging from personal revenge, corrupted employees, group of attackers with no intention, organized crime paid with particular target to mentioned espionage on national level. Following picture divides attackers into 4 basic groups with description of their targets, their motivation and impact.

Picture 1: Profile and division of cyber attackers



	Motives	Targets	Impact
Nation State	economic, political and/or military advantage	Trade Secrets, sensitive business information, emerging technologies, critical infrastructure	Loss of competitive advantage, Disruption of critical infrastructure
Organized Crime	immediate financial gain; collect information for future financial gains	Financial systems, personally identifiable information, payment information, health information	Costly regulatory inquiries and penalties, Loss of confidence
Hacktivists	influence Political and/or social change; Pressure business to change	Corporate secrets, sensitive business information, personal information	Disruption of business activities, Brand and reputation
Insiders	Personal advatage, monetary gain, professional revenge, patriotism	Sales, deals, market strategies, corporate secrets, business operations	Trade secret disclosure, Operational disruption, National security Impact

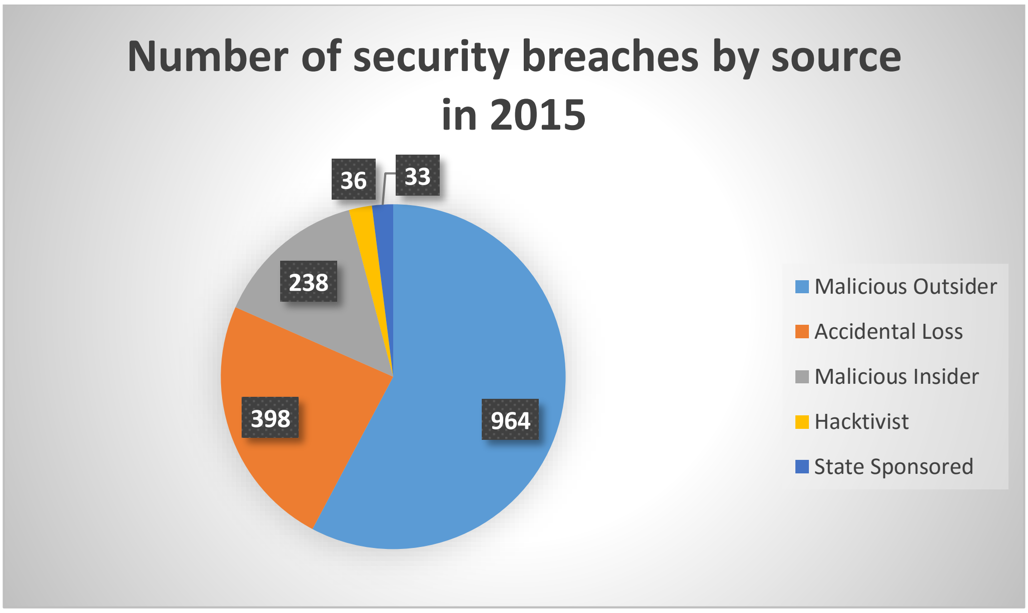
Source: PwC, Cyber Risk A Threat to Energy Security, edited by author

Insiders or in other words people working in the given organization are only group representing the internal threat in organization, which is in past years on upraise. The motivation of the employees can have a negative motive for personal monetary gain or revenge to the employer for personal clashes or other reasons. Part of insiders group that is not identified and described in this table represents ones with lack of experiences and knowledge in IT acting uncounciously harmfully. Such users have no intentions at the very beginning.

Other 3 groups included in the table represent the adversary actors outside the organization. One feature that is in common across all groups is endeavor for own benefit in financial means, advantegous position to another organization/person or enforcement of own political/economical thoughts and ideas through malicious tools. Two groups that the organizations should be aware of are organized crime and nation state which might have the biggest impact on targeted organizations. Unfortunately in case of governments as a target of cyber crimes, all four groups are relevant potential sources and should not be underestimated. Altough question of cybersecurity is still woefully underestimated as a potential risk factor. According to Freshfields survey from 2014 of 200 global dealmakers, 78 percent of respondents said that cybersecurity was not analyized in great depth or specifically quantifies as a part of the typical Merge and Acquisition process due to diligent process.

Distribution and percentages of defined groups of attackers was carried out by company Gemalto showing recent frequent sources of attacks in data breaches.

Table 1: Sources and number of attacks in data breaches 2015

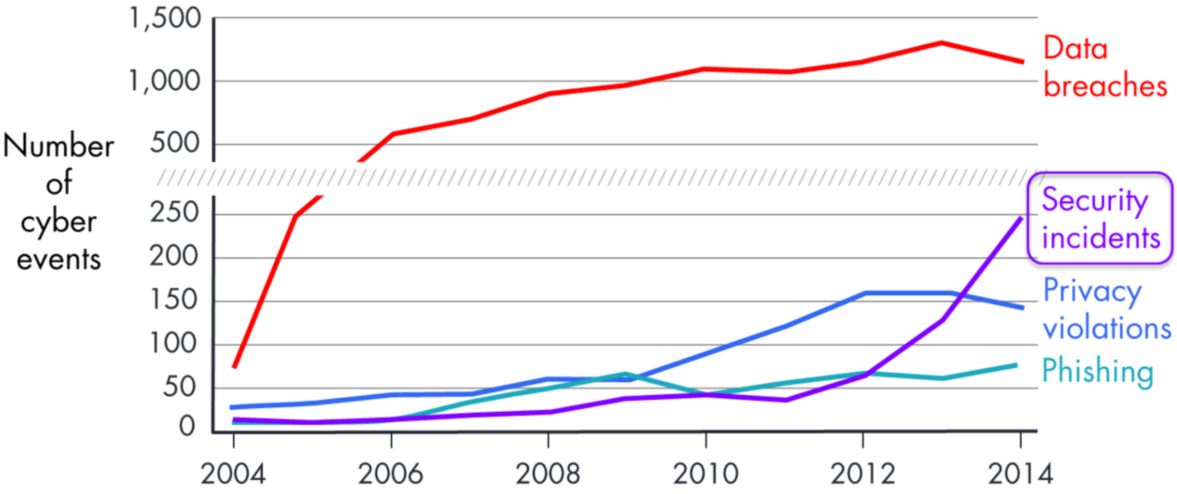


Source: Gemalto, Breachlevelindex.com, edited by author

If cyber criminals can thwart the best efforts of Western governments and corporations, then doing business in Africa presents particular risks. There are insufficient laws and regulations across the continent that recognize the pervasiveness of cybercrime and prescribe clear penalties for offenders. The cyber skills of law enforcement agencies, governments, and private sector organizations are low, while security controls at the personal, institutional, sectoral, and national levels are largely absent. [38]

The legislative and regulatory measures were already introduced and described in previous part of Analytical Part as a core and supportive element necessary to further develop cyber security accross Member States. However the practical areas where the cyber incident occur was not broadly covered and defined in the Convetion, leaving the space open and up to every government. Trend of attacks comitted on goverment agencies in past 10 years is shown in following graph

Graph 4: Type of attacks compromising government agencies



Source: Law Enforcement Cyber Center 2015

Recently examined dataset of over 12,000 cyber incidents that occurred during the years 2004-2014. These events include data breaches (unauthorized theft or loss of personal information), privacy violations (unauthorized collection or use of personal information), security incidents (hacks directed specifically at an organization), and other sorts of phishing or identity theft scams. [39]

Dataset reveals us the intentions behind the attacks where the great part accounts for unauthorized theft/access and loss of personal infromation. Reasons for that are not further specified but is a part of the suggestion part to cover most frequent and harmful scenarios. This group is followed by growing number of security incidents of hackers aimed on a

[38] MULLIGAN, Helen a Owen O'RORKE. *Bloomberg: World Data Protection Report,* The Growing Threat of Cyber Attacks in Africa

[39] Cyber incidents against government agencies. *Law Enforcement Cyber Center*

organization with specific task, for example, to gain certain information. Privacy violations is a part covered in the convention reffering to neccessary time to keep particular information for given process, where in other cases should be such information properly stored, secured and erased. This problem is already addressed and being on decline thanks to adequate set up framework for processes. The importance of framework for processes, managing risks and control over the own assets was further described in Bloomberg World Data Protection report in following formulation concluding this chapter of Analytical part.

Good cyber governance is about more than just technology. It's about managing behavioral risk, as Edward Snowden and Chelsea Manning, reports from professional services networks and cybersecurity firms, and massive breaches such as Target and Morgan Stanley, highlighting the threat from within (employees and vendors), have shown. Tackling this in Africa is a monumental challenge. The continent is prone to corruption, providing 15 of the 30 worst offending countries in Transparency International's 2014 Corruption Perceptions Index. Other aspects of the behavioral problem are illustrated by one of the classified files passed to Al Jazeera — a South African intelligence report entitled ''Security Vulnerabilities in Government.'' The file lists laptop thefts, unencrypted communications, and limited vetting of senior officials as some of the reasons why the government is so vulnerable to spying. With valuable data at stake, businesses should also guard against internal dangers. [40]

Moreover it is a cornerstone to have a secure and transparent state sector, to quote Melissa Hathaway, cyber security consultant of George W. Bush and Barack Obama: "*Cyber threat is one of the most crucial problem in economic and state security that we face as a state."* She concluded many examples how cyber criminality and other related threats negatively influence HDP.

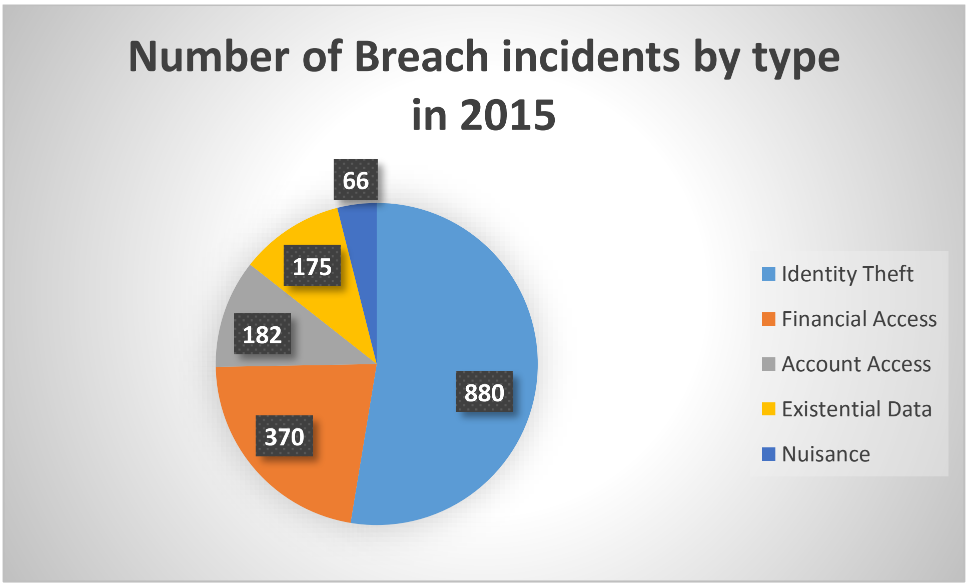
2.5.4. Number of information compromised

After identification of very basic division of different type of attackers in cyber world will be examined numerous examples of information losses around the world and on example of South Africa. Motivation behind every attack was briefly described in previous chapter and the aim of the attacker may vary. In general can be said that the attacker seeks and attempts to obtain certain information either for his personal use/abuse or was paid by 3rd side for their

[40] MULLIGAN, Helen a Owen O'RORKE. *Bloomberg: World Data Protection Report,* The Growing Threat of Cyber Attacks in Africa

personal benefit. According to Gemalto, total number of records breached in 2015 peaked on number 707 million records in 1673 registered breach incidents. Comparing to previous year the number of 1 billion records accessed by unauthorized person is significantly lower, however this number is very fluctual due to the fact that registered attacks are taken into account. One characteristic relevant for data breaches in 2015 their personal character.Type of the stolen records is shown in following graph.

Graph 5: Data breached in 2015



Source: Gemalto 2015, The Year of Data Breaches Got Personal, *edited by author*

Types of various records that are aimed in data breaches are broad and it is always hard to cover greater part of such information collections assessed as sensitive or neccessary to protect. For this purpose will be described few examples around the world including South Africa to prove the diversity of aimed infromation during cyber attacks.

First example comes from insurance companies from US, where the attack against U.S.-based health insurer Anthem was an identity theft breach that resulted in the theft of 78.8 million records, making it the largest data breach of the year in terms of records compromised. The breach scored a 10 on the risk assessment scale [41]

The company declared that attacks were made on its IT systems to get private information about individuals with data from Anthem Systems. The information content was related to

[41] *Gemalto: 2015, The Year Data Breaches Got Personal*

health plans of current and former member of Anthem's affiliated healthplans and other independent companies‘ plans. Investigators suspects that the breach was sponsored by other state. Certainly information about one's health plans can have fatal impacts in case that their adversory or person with personal revenge motivation gets control over them.

An example of successful data breach concluded by malicious insider comes from South Korea, saying the South Korean organization, which distributes pharmacy management software to many of the country's pharmacies, was hit by an identity theft breach launched by a malicious insider. The result was the exposure of 43 million records, and the incident scored a 9.7 on the risk assessment scale. According to the Korea Herald, medical information on nearly 90% of the South Korean population was sold to a multi-national firm, which processed and sold the data. [42]

Seriousness and wave of uncertainty coming from alienating personal information of citizens was witnessed in USA in Office of Personel Management. The OPM in June 2015 suffered an identity theft data breach that involved 22 million records. The state-sponsored attack, which was described by federal officials as being among the largest breaches of government data in the history of the U.S., scored a 9.6 on the risk assessment scale. The attack exposed data including personally identifiable information such as Social Security numbers, names, dates and places of birth, and addresses. [42]

Last example comes from South Africa where company Gemalto brought an insight in question what organization has been targeted since 2013 in South Africa suprisingly mentioning police. South Africa had nine significant breaches between the start of 2013 and today.

The most-targeted organisation was the South African Police Service, which came in at the number one spot with the loss of 15 000 personal records. The source of the breach were malicious outsider(s) and they were after data that could be used to steal identities, according to the report. [43] Other minor attacks were conducted on WooThemes and WordPress where the stolen data according to the companies were financial information.

All described cases from different part of worlds and industries represents a minority of attacks that were conducted during the last year and the number is still on the rise. Techniques and level of knowledge neccesary to make a cyber attack agaisnt any subject is dropping

[42] *Gemalto: 2015, The Year Data Breaches Got Personal*

[43] *HTXT Africa: POLICE DATABASE HACK TOPS LIST OF SA SECURITY BREACHES*

lower by every year thanks to the information availability in today’s world and technical means publicly available. The size and power is irrelevant in this case to commit a cyber attack agaisnt a subject of matter size which leaves out traditional obstacles like borders, armies, power and other factors. This represents a great threat to every individual and organization in the state or region.

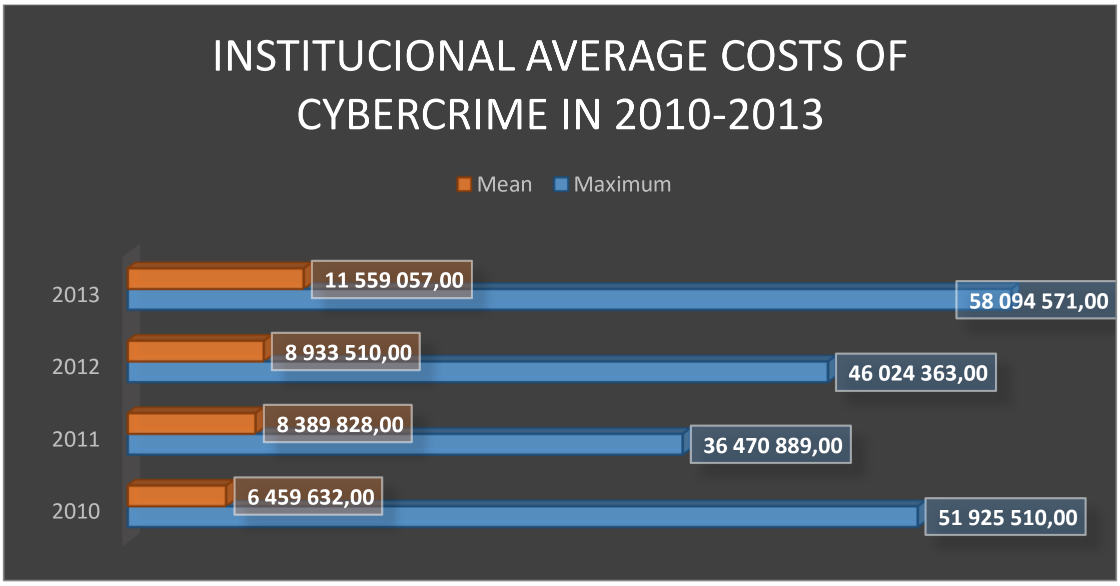
2.5.5. Calculation of Costs of Cyber Crime

In previous chapters were identified briefly the question of what does it mean to be vulnerable to cyber threat, what are the basic groups of malicious attackers aiming to commit a cyber attack on an organization and lastly have been showed what are such cyber attackers targeting for to obtain via those attacks. Last and for point of regional development most important point is dedicated to calculation of such attacks. Attacks are threatening the organization or individual’s personal and sensitive from which the major budget bearing costs come from – lose of competitiveness, alienation of sensitive information about certain process, personal information, financial records and information and other relevant information. The additional costs come also after the incident occurs, putting extensive work pressure on IT department, administrative and regular employees temporarily unable to access a service, profit loss during that time, availability of public services disabled and so forth. Those estimations of extra costs do not include those incidents that have not been registered by the organization thus the numbers show up the lowest costs burden possible.

Organizations lose billions of dollars each year due to cyber-attacks. The sheer amount of sensitive data that’s openly available on the web today is making it increasingly difficult to combat these cyber threats. The benefits of using a cyber threat intelligence platform can drastically outweigh the danger of not doing so. Per the 2013 Costs Cyber Crime Study by the Ponemon Institute, the average cost of a cyber-attack is more than $1,000,000 and takes 32 days to resolve. So that’s more than $32,000 per day to find and resolve a typical cyber-attack. The figure below shows annualized costs of cyber crime. The median in 2013 was $9.1m, an increase from $6.2m in 2012. [44]

[44] *IKANOW: Cyber Threat Intelligence Platform: What are the threats not implementing one?*

Table 2: Calculation of cyber crime annually in years 2010-2013



Source: IKANOW 2014, Cyber Threat Intelligence Platform, edited by author

Provided table shows us the progressive trend in terms of costs of cybercrimes, it's minimum and maximum limits with mean values as well. Inspecting data closer each value will indicate that minimum costs of cybercrime in average annually costs about 1 million dollars. The value has not changed much during the period of four years, however the situation starts to change a bit while examining average numbers together with maximum costs related to cyber attacks, reaching in average 11 million dollars with still growing trend peaking on the number of 58 million dollars for year 2013. The minimum costs correspond to attacks that were registered by the organization and were in certain way solved – or there was an attempt to solve out.

It could be argued that the question of costs of cyber crime is yet not related to African countries as up-to-date topic. But just right because of increasing number of used devices connected to internet, computerazing of government faciliets, networking their whole structure reliying on internal systems which they daily work on, all these factors represent a huge threat to local facilities. One practical example from calculations and comparisons of cyber crime in South Africa comes from Bloomberg, talking about South Africa as a hub for cyber attacks as well as a target of attackers.

Africa accounts for 10 percent of global cybercrime incidents, with Kenya, Nigeria and South Africa identified as growing hubs of criminal activity. So far the data collected by Symantec, global leader in developing security software, reveals that only Russia and China have more victims of cybercrime each year than South Africa. Cyber Attacks costs the country about 5.8 billion rubbles, which is approximately 500 million dollars every year with recent strikes on instutions including Gautrain Management Agency, Postbank, the governing African National Congress and country's police service. On average it takes South African organizations to track the origion of the attack about 200 days, until then attacks remain unnoticed. [45]

Other example from Central Africa from Nigeria refers to similar situation, where data breaches rose by 62 percent in 2013, and both Deloitte and Cisco have warned the country it is at risk of a major attack. In January, the website of Nigeria's Defense Headquarters was compromised in an ‘‘ISIS-style attempt’’ to hack into government platforms. Cisco singled out Nigeria's banks, oil and gas companies, and government as being particularly vulnerable. [45]

Another relevant source MacAffee, world leading producer of security software, have carried out a document estimating global cost of cybecrime. Besides elaborated data sets that will be presented in following tables, they have mentioned an important fact saying that the hardest estimation of costs of cybercrime is in case of stolen intellectual property which again points on fact that cryptography tools should be widely used for different types of sensitive documents. First table shows us comparison of costs of different unlegal and budget-burden activities in global measure:

Table 3: Financial burden of activities in % of GDP

Activity	Cost as % of GDP
Maritime Piracy	0.02% (global)
Transnational Crime	1.2% (global)
Piracy	0.89% (global)
Narcotics	0.9% (global)
Cybercrime	**0.8% (global)**

Source: Net Losses: MacAfee, Estimating the Global Cost of Cybercrime 2014, edited by author

Following data shows us that Cybercrime among other different areas that are perceived as important to resolve present a huge threat on uprise with expecting increasing number in following years. Important note is that the estimation counts for cases that have been

[45] MULLIGAN, Helen a Owen O'RORKE. *Bloomberg: World Data Protection Report*, The Growing Threat of Cyber Attacks in Africa

registered and confessed by the subject. Global justification for awareness and importance of this topic by organizations, states, companies and other institutions is then on place.

According to BusinessTech websites, Cyber-crime is having a significant economic impact on South Africa and the rest world, costing the country over R5.8 billion each year, approximately US$550 million – a situation set to get worse. [46]

Another table is showing calculation of cybercrime as % of GDP for states that will bring our topic and cost estimations of cybercrime closer to South Africa.

Table 4: Costs of cybercrime in % of GDP by country

Country	% of GDP
Australia	0.08%
Brazil	0.32%
Canada	0.17%
China	0.63%
Colombia	0.14%
EU	0.41%
France	0.11%
India	0.21%
Kenya	0.01%
Mexico	0.17%
Nigeria	0.08%
Russia	0.10%
South Africa	**0.14%**
Turkey	0.07%

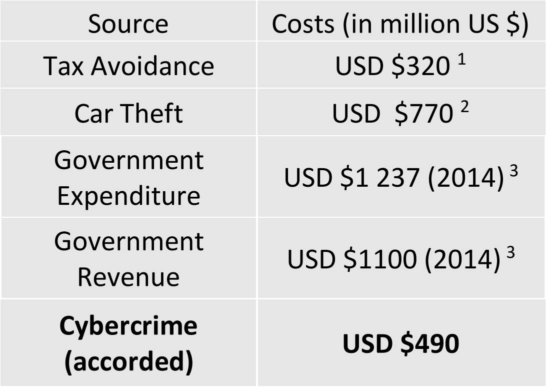
Source: Net Losses: MacAfee, Estimating the Global Cost of Cybercrime 2014, edited by author

Observing the data set South Africa's value of 0.14% GDP in 2013 belongs to the average number among the examined states where the highest percentage is about 1.50% of GDP in Germany. The amount of GDP and thus the absolute numbers differs from state to state according to the percentage burden and gross domestic product output. In case of Africa to latest data from Trading Economics in years 2011 – 2014, South Africa reached GDP starting at US$416.6 billion to US$350.085 billion respectively. By simple calculation the average cost of US$582 million to US$490 million annually respectively. To project this amount of costs of cybercrime to government annual revenues, it represents approximately 1% of state revenues from total amount of 65 billion US dollars in year 2014 which is equal to annual

[46] The cost of cyber-crime in South Africa. *BusinessTech*

costs of car thefts in South Africa. Comparison of other extra budget burden costs is allocated in following table:

Table 5: Annual cost comparison of different activities



Source	Costs (in million US $)
Tax Avoidance	USD $320 [1]
Car Theft	USD $770 [2]
Government Expenditure	USD $1 237 (2014) [3]
Government Revenue	USD $1100 (2014) [3]
Cybercrime (accorded)	**USD $490**

Sources: [47] Africa Business Review 2012, Tax Evasion costs; [48] Bloomberg 2014, Car Theft and Hijacking Costs, [49] National Treasury Republic of South Africa 2015, Budget Review; Edited by author

Different areas of activities with negative impact on state budget or state budget balance itself shows us in the comparion with the costs of registered and confessed cybercrime events that total amount among other problems is definetely not negligible. As the recent registered attacks compiling in the amount of 490 million USD was comitted on government and state-ruled bodies, than in simple comparison we can observe that almost half of the cybercrime costs in year 2014 was almost half of government expenditure.

However the real costs of cybercrime still does not provide comprehensive assumption of the expenses as the most important part, intellectual rights and property, don’t have yet any appropriate formula or assessment explaining the real value of certain information. As the value of the information cannot be assessed and the real value of the information is relative in time and space, it is a core part that will always miss from the estimations. To explain dilema with intellectual property can be described a situation from technological environment, where company A real value of certain knowledge about certain product might consist of the money invested in reasearch and yet discovered facts, where as company B, which might utilize this information could get a absolute advantage on market which would result in performance downgrade for company A. Similar situations can be performed on examples of governments

[47] Tax evasion costs South Africa 'billions'. *African Business Review*
[48] Car Theft and Hijackings South Africa. *Bloomberg*
[49] Budget Review. *National Treasury Republic of South Africa*

in international field in gaining advantegous positions thanks to accessing secret information etc.

According to recent changes in African Union Convention on Cyber Security and Personal Information Protection the extra costs and punishments will arise from unability of the official bodies to secure sensitive information, resulting in extra budget burden for Member States if investigation proves that the standards have not been met and followed. However another costs resulting from cybercrime such as calculation of stolen intellectual property or breaches that have not been registered and thus not included in the costs are missing in the estimations which shows that presented costs will count for the lowest possible costs.

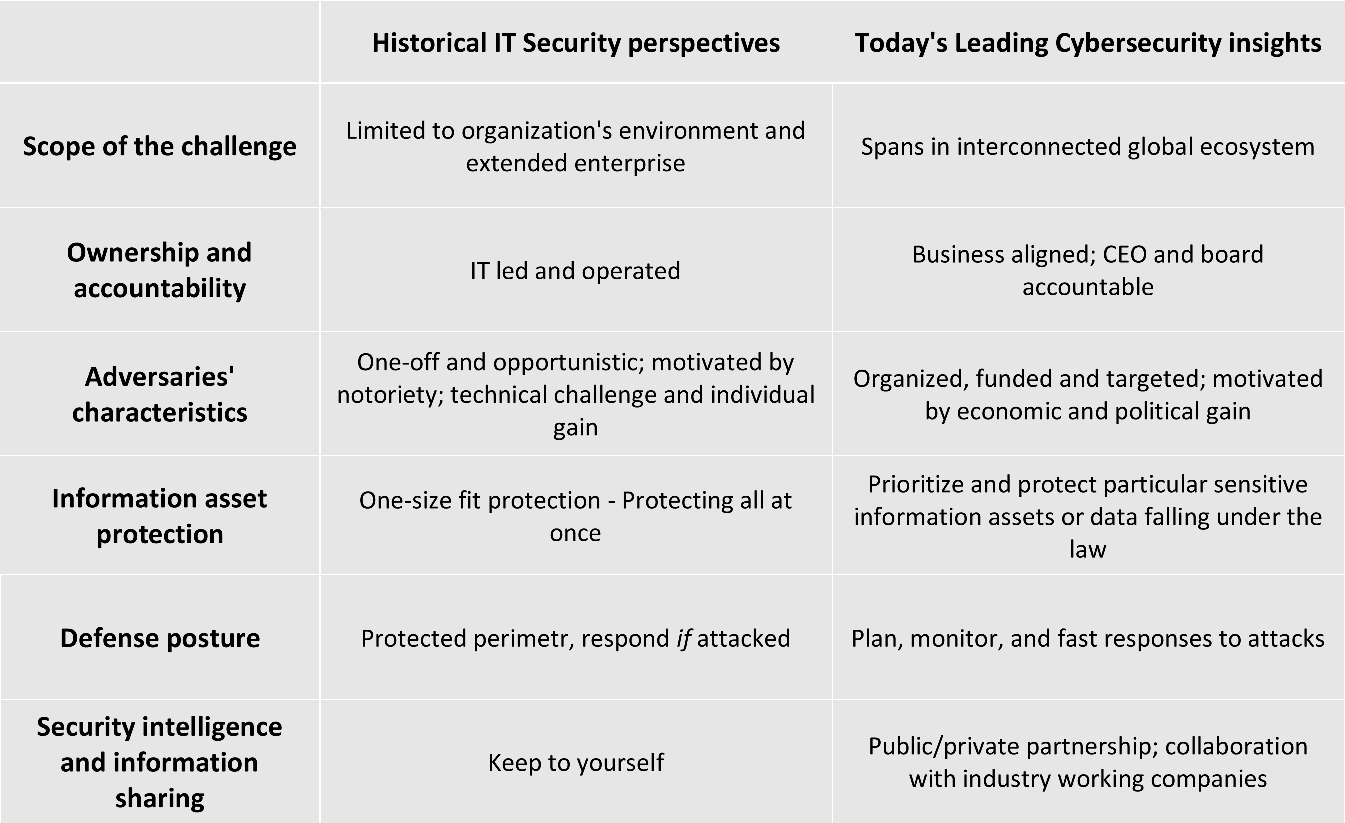
3. Suggestion Part

First chapters of analytical part were allocatingnd information related with protection of personal information and cyber security issues with comprehensive framework in legal and regulatory aspects providing a solid milestone for every commited Member State to follow. Criminal provisions for individuals and organizations committing crime against set up points in the Convention have very broad coverage of different scenarios to avoid any misunderstanding and misinterpretations of cyber crimes and crimes with profileration of personal information against current law which should result in adequate sanctions and punishmenet for such crime. On the other hand practical insights how to assess organization’s situation and what necessary steps should they undertake to reach certain level of security standards has very general interpretation leaving this question up to every Member states will and best intention. This concept of basic security standards is part of suggestion part where I have collected information and experiences gained in the field of cyber security on subjects in Czech Republic, either in public or in private sector.

Case studies themselves show us only statistical data from states of different regions and also on examples from Africa, giving us absolute numbers what are the costs of cyber incidents starting from early stage to post-incident stage with recovering to the initial stage before attack occurred. It can also be stated that based on the number of attacks in recent years, variables like increasing number of smartphones, computers, systems reliable on information technologies (digitalizing), higher number of unsecured wireless access points etc., that concerning about cyber security in wider range, particularly in case of governmental and private sector is at the place. As it was shown the typical targets of attacks are in recent year technical industries, financial organizations and state bodies on the top, providing sufficient justification for actions taken by public and private bodies.

Another data chart presented in analytical part looked at different type of attackers, their motivation and whether they were insiders or outsiders which should help the organization to determine bottlenecks in security and to develop a better security proposal based on own carried out analysis. This information should server for further decisions on what to focus in terms of control over information and their security in order to control, analyze and prevent any unlikely scenarios. The recent trends in security attitude is shown and described in following graph:

Graph 6: Security trends in recent years



	Historical IT Security perspectives	Today's Leading Cybersecurity insights
Scope of the challenge	Limited to organization's environment and extended enterprise	Spans in interconnected global ecosystem
Ownership and accountability	IT led and operated	Business aligned; CEO and board accountable
Adversaries' characteristics	One-off and opportunistic; motivated by notoriety; technical challenge and individual gain	Organized, funded and targeted; motivated by economic and political gain
Information asset protection	One-size fit protection - Protecting all at once	Prioritize and protect particular sensitive information assets or data falling under the law
Defense posture	Protected perimetr, respond *if* attacked	Plan, monitor, and fast responses to attacks
Security intelligence and information sharing	Keep to yourself	Public/private partnership; collaboration with industry working companies

Information obtained in the chart reveals us past trends related with cyber security and modern attitude with leading insights. Probably the most important point of the table is the information explaining “defense posture”, which has changed in recent years from only protecting own perimeter to monitor, control, plan and respond to events occurring in internal site, such as connection of non-authorized USB devices, handling important documents elsewhere, browsing dangerous websites etc. Many of those actions done by internal employes are potential open doors for malicious outsiders in general.

The suggestion part will however begin from the fundemental steps where should every single organization start with. It’s not very propable that any person from the organization could clearly say in which concrete parts they see a problem. Any implementation of software means and other regulations should be preceeded by analysis - in our case, analysis related with security and productivity. No one should rely on studies carried out by companies on different subjects as every subject has different environment, structure, rules etc. This is why it is recommended before any radical and costly decisions to perform risk and personal audits that will appoint on most alarming gaps. Processes to be taken will be described in following chapters.

3.1. Description of the Cyber Security Concept

The goal of suggestion part of this diploma thesis is to propose a basic rough Cyber Security Concept that has been generally described in African Union Convention on Cyber Security in order to achieve information security of the organization against internal and external factors and promote sector effectivity and control over assets by various technical means that are to be described in following steps. It is important to realize that increasing number of incidents and cyber attacks might have cause in of unconscious and unresponsible behavior of users with information technologies in/out organizations perimetr that creates temporary gap that can be abused. Following solution deals with data security and effective use of IT resources that also come up with preventive security measures to control internal processes and data in the environment of the organization.

This Cyber Security Concept is meant to be a potential guideline for Member States of African Union, particularly for South Africa and related cooperative partners, in the matter of cyber security field to encourage the basic standards of security measures set up in African Union Convention on Cyber Security. Application of such concept will ensure the organization security of information, increase control over own assets, effective use of own resources, both IT and financial. By promoting basic security and control management measures the organization is preventing any further problems in case of loss of information, post-recovery stage of cyber incidents, effective use of own resources that will positively result in financial savings for further development of other important sectors of the state. Such precautions will be predominantly done by encryption of data that will be recognized in risk analysis as critical and sensitive, increasing the current range of information that are obligatory to secure according to legislative requirements.

3.2. Processes to be taken

3.2.1. Risk analysis

Risk analysis is a very complex document based on collaboration of professional IT company dealing with cyber security and customer that looks on processes of handling of data in the organization. It consists of work with the IT means (computers, laptops, servers, firewalls, USB, phones etc.), prescribed steps while processing certain documents (business contracts, plans, budgets, personal information, accountancy, construction procedures), electronic communication procedure and their preserving/securing from possible external threats. Outcome of the risk analysis defines current situation of organizations flow of information in the network and suggest changes in the framework and helps to implement changes in internal structure to promote secure movement of data. To mention some of the outcomes, risk analysis defines data sensitivity according to their content and importance, calculate a potentional financial loss from probability and total amount of financial loss varibles. Information are afterwards divided into four groups public, confidential, senstivice and critical information, defining borders and routes where the data can move eliminating the necessary presence of the information in their target storage. Besides the movement borders of information is defined as well necessary time of such information to be present in network accessible from local network or internet to eliminate any unintended access of employees, malicious insiders or outsiders. Any further details of the process itself with specific steps are subject of the risk analysis thus cannot be specifically described in this concept. Together with the document from Internal Personal Audit organization can evaluate data that are necessary to secure and is on a right path to implement any software measures to encrypt critical information data sets.

3.2.2. Internal Personal Audit

Such audit is done predominantly executed by the IT company with initial collaboration with the customer where the necessary tools are implemented in the organization to monitor the daily routine of employees and movement of the data. This step was discussed already in graph 6, showing cyber security trends of past and present, where monitoring, evaluating and reacting was emphasized as essential part of modern approach to security. Such audit looks on application usage, visited websites, work with particular data, use of printing means, work with external devices, HW/SW audit etc.

The activities have two dimensions – economical and security one. Economic reasons are obvious to look on utilization of work time and work means in order to lower the costs. Security then looks on movement of the data, their handling, storing, printing of sensitive documents, monitoring of dangerous websites, plug in/out of unauthorized external devices etc. Result of the audit will show on actions, work and rules discipline of users where the important information will rely on handling the data, access to data, access to dangerous websites, external devices, e-mail and their attachements/content, and lastly HW/SW use for optimization. The outcome of the audit based on those infromation is to determine further future necessary implementation steps of software solutions for better control over own assets, better economic efficiency and implementation of encryption tools on necessary information in the organization to prevent potential dangerous behavior of the user on the end-station and in network to prevent further damage of the internal structure of the organization leading to loss of data, upload of malware etc.

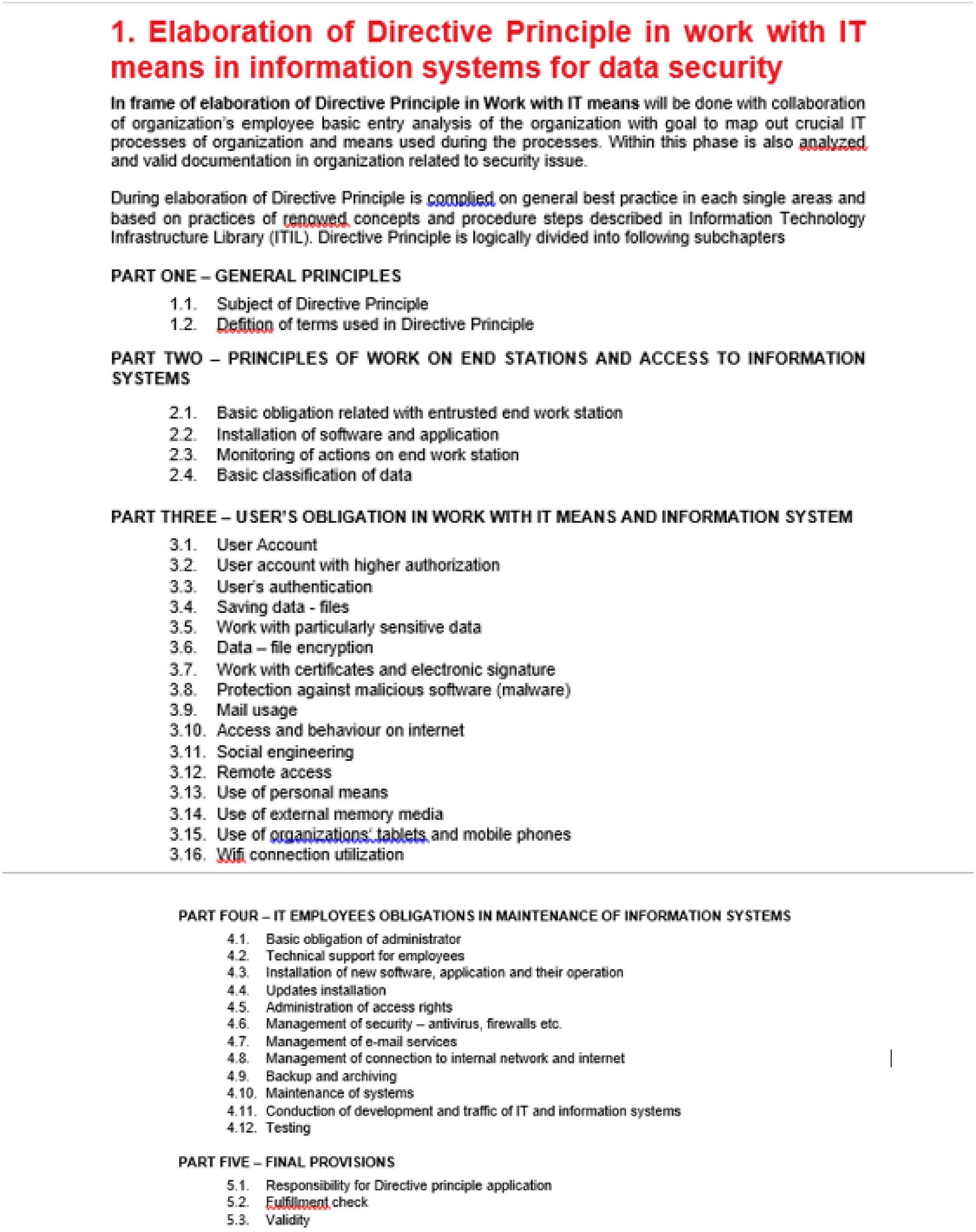
3.2.3. Security measure design proposal - Directive of work measures in IT

Following document is carried out based on results from risk analysis and Interna Personal audit summarizing rules and guidelines to be followed while working with IT means in organization and prevention of possible incidents harmful to organization. The Directive of Work with IT covers is a broad concept of basic rules from various password types used (for example “do not use same password in company account as user have on social sites”) handling and saving of important documents on determined locations, avoid unconscious dangerous behavior of users during their work with IT means.

These steps should bring users a bit closer to dilema of cyber security, give them the idea of awareness while working on PC and to transfer responsibility and accountability on end user. Besides the directive for all employees the output will also make additional changes to IT structure and framework of operating within the organization in order to promote more secure steps. This step is done in accordance and by customer's desire and needs. This pre-step is covering changes in operational aspect in order to avoid basic possible threats by changes in the processes. In case of further gaps in security and use of IT means based on risk analysis and Personal Audit are recommended further steps in SW implementation to fill those shortcomings and to eliminate user mistakes and dangerous behavior.

In ideal situation the Information Technology sector should be divided into security and operational department to divide and separate those 2 branches a part to avoid any confusing conclusions. IT operational department has a goal for fluent and smooth working of IT means where is IT Security department should look over the best practices of the users to maintain the information secure and network compact and integrated without any breaches. Such step was also supported in African Union Convention saying that National Authorities should establish Cyber Security deparment working independently from others to ensure set up standards in the Convention. Outline of such Directive of Work with IT means can be seen in following table of content of the document.

Picture 2: Table of Content of Directive of Work with IT means:



1. Elaboration of Directive Principle in work with IT means in information systems for data security

In frame of elaboration of Directive Principle in Work with IT means will be done with collaboration of organization's employee basic entry analysis of the organization with goal to map out crucial IT processes of organization and means used during the processes. Within this phase is also analyzed and valid documentation in organization related to security issue.

During elaboration of Directive Principle is complied on general best practice in each single areas and based on practices of renowed concepts and procedure steps described in Information Technology Infrastructure Library (ITIL). Directive Principle is logically divided into following subchapters

PART ONE – GENERAL PRINCIPLES

1.1. Subject of Directive Principle
1.2. Defition of terms used in Directive Principle

PART TWO – PRINCIPLES OF WORK ON END STATIONS AND ACCESS TO INFORMATION SYSTEMS

2.1. Basic obligation related with entrusted end work station
2.2. Installation of software and application
2.3. Monitoring of actions on end work station
2.4. Basic classification of data

PART THREE – USER'S OBLIGATION IN WORK WITH IT MEANS AND INFORMATION SYSTEM

3.1. User Account
3.2. User account with higher authorization
3.3. User's authentication
3.4. Saving data - files
3.5. Work with particularly sensitive data
3.6. Data – file encryption
3.7. Work with certificates and electronic signature
3.8. Protection against malicious software (malware)
3.9. Mail usage
3.10. Access and behaviour on internet
3.11. Social engineering
3.12. Remote access
3.13. Use of personal means
3.14. Use of external memory media
3.15. Use of organizations' tablets and mobile phones
3.16. Wifi connection utilization

PART FOUR – IT EMPLOYEES OBLIGATIONS IN MAINTENANCE OF INFORMATION SYSTEMS

4.1. Basic obligation of administrator
4.2. Technical support for employees
4.3. Installation of new software, application and their operation
4.4. Updates installation
4.5. Administration of access rights
4.6. Management of security – antivirus, firewalls etc.
4.7. Management of e-mail services
4.8. Management of connection to internal network and internet
4.9. Backup and archiving
4.10. Maintenance of systems
4.11. Conduction of development and traffic of IT and information systems
4.12. Testing

PART FIVE – FINAL PROVISIONS

5.1. Responsibility for Directive principle application
5.2. Fulfillment check
5.3. Validity

Source: Sodat Software 2015, Směrnice zásad práce, edited by author

3.2.4. Software implementation

Following step is based on evaluated data from both, risk analysis and personal audit to implement the SW solutions in the most suitable and effective way. In the decision making should be also taken into account requirements and regulations from African Union Convention on Cyber Security and best sector practices to achieve basic security standards with, control over own assets and economic efficiency of the organization in terms of IT means. Such solutions include file encryption on laptops, mobiles, USB devices, file servers and tablets with a secured communication canal called as save mailing. The need, simplicity and effectivity of encryption of information was further supported by Gemalto company informed on website htxt.africa saying following statements about use of encryption tools and their effectivity when it comes to security:

Gemalto has also put together a fascinating infographic on the site, which illustrates all of 2014's recorded breaches from across the globe. Just over a billion records were "lost or stolen" over the year, apparently, but most importantly, the infographic stresses that only four per cent of all hacks were of "secure breaches", meaning the theft of encrypted data that ultimately proved useless to the thieves. That's actually the point the site stresses over and over: that better data security policies are highly recommended, and that encryption should be deployed across all organisations' datacentres in order to render any stolen data useless to hackers. Gemalto also emphasises that companies should no longer favour an "if" mentality when it comes to being hacked, but a "when", and instead adopt policies focused on how to "Secure the Breach". [50]

Such solution will prevent other unauthorized users, malicious insiders and outsiders either from the organization or external citizens to access, read and abuse the data. Such encrypted data prevent from further abusement of the information in the documents, contracts, personal information etc. and prevent a huge problem solving to organization stemming from alienation of personal or internal organization information that are extremely costly. The encryption tools should be however used across more sectors than it was specified in National Cybersecurity Framework of South Africa to cover wider range of information such as personal information, offline mail inbox, sensitive documents on users' computers, and so forth. However the whole encryption coverage of information is subject of risk analysis described in suggestion part.

[50] *HTXT Africa: POLICE DATABASE HACK TOPS LIST OF SA SECURITY BREACHES* [online]. 2015

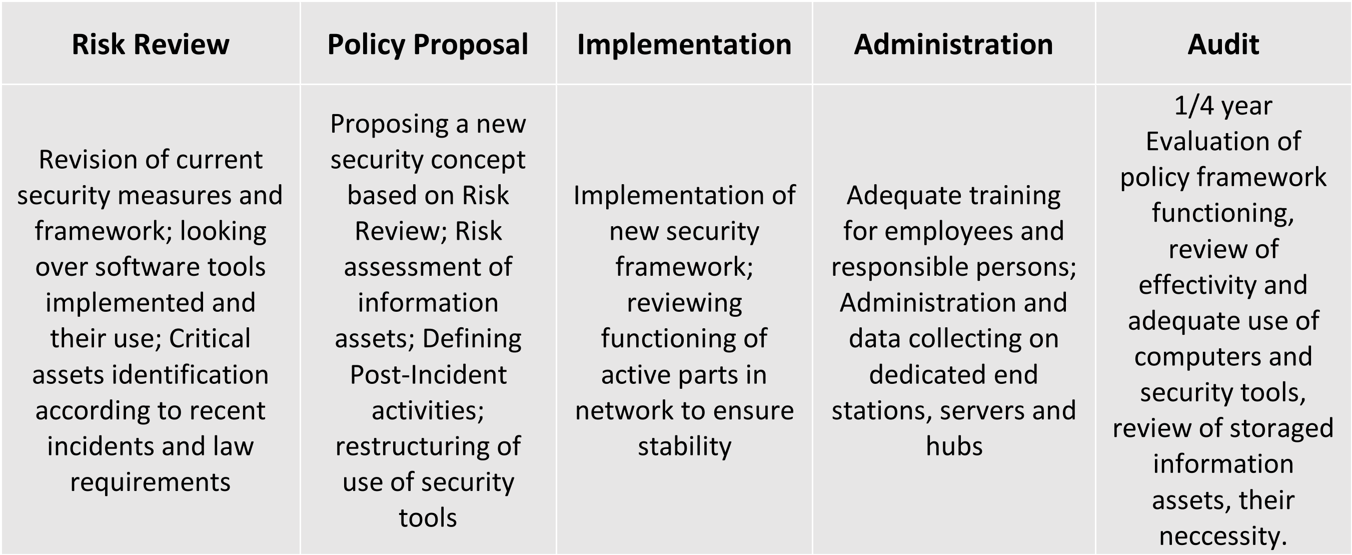
Other tools used cover the economic and security aspect at once. Their application may be applied on end stations, terminal servers and traffic hubs that look over and analyze movement of information, documents, behaviour of the user on the endstation, printing sessions, mailing communication with important attachements, use of HW/SW means on the end stations. Software solutions always come with sophisticated evaluation and alert system to warn about unwilling actions. So called "anomalious behaviour of user" in above mentioned categories is carried out by the software means itself, saving time of the responsible persons and also give a possibility to restrict dangerous behavior acts in order to preserve organization safety and functionality. Tracking and evidence of incidents that targeted certain information can be also used in judicial processes as evidence what was the target and aim of such attack. Courts and law does not often recognize content of the information in cyber sphere as relative subject to judicial process due to evidence and proof of any attacks. Such implemented tools should facilitate this process.

These preventive solutions for encryption of information and monitoring with analysing tools helps organization to see their cyber incidents in advance, giving adequate tools to track the source of such cyber incident, which will positively reflect in saving of extra financial burden to resolve such situation that can result from users unaware behavior and security gaps in organization security wall. Above described tools also promote better use of organization assets, including time, employees and technical means by continual check in utilization of such working tools giving organization great preview of economic management of organization.

3.2.5. Monitoring and revision for sustainability

Last step is partly a key for sustainability of the whole idea Cyber Security Concept. This does not necessarily mean that without monitoring and revision the aim of the proposal would not enhance today's situation in public and private sphere but is a key to keep up with modern trends and problems in area of cyber security. In order to implement, use and utilize the technology in most effective manner is recommended to revise current situation once in a half year or one year to see in what areas have been made a progress so far and which need more attention and additional changes. The reason for that is obvious. Network, end stations and users and surrounding environment do not have static status and is changing every day. It shifts over time and this has to be reflected also in policy settings, technologies used in organization to handle the situation in the best possible way. Such process can be seen on following pictures XX and XX, showing more descriptive reasons in respective area and basic lifecycle of cyber security.

Picture 3: Security process steps



Risk Review	Policy Proposal	Implementation	Administration	Audit
Revision of current security measures and framework; looking over software tools implemented and their use; Critical assets identification according to recent incidents and law requirements	Proposing a new security concept based on Risk Review; Risk assessment of information assets; Defining Post-Incident activities; restructuring of use of security tools	Implementation of new security framework; reviewing functioning of active parts in network to ensure stability	Adequate training for employees and responsible persons; Administration and data collecting on dedicated end stations, servers and hubs	1/4 year Evaluation of policy framework functioning, review of effectivity and adequate use of computers and security tools, review of storaged information assets, their neccessity.

Sustainability is from a certain point of view question and matter of Cyber Security Life Cycle ensuring up to date security measures. To maintain policies actual is required and expected proactive approach of the South Africa’s government bodies with provider of software security tools to react on the government actual needs. The technologies themselve do not mean anything without proper training and maintenance, that is also covered in the life cycle of Cyber Security, providing trainings for local staff by supplying company for adequate training by software developers to bring out the best possible outputs, utilization and news related with the software tools. This is important point in the whole idea to ensure the ability of the organization to operate with the systems, software means, adjust desired changes according to their will, see the value in the data coming out from the tables and to be able to do their own analysis with the tools available in the software solution. The ongoing process of changing needs in terms of cyber security was already stressed out in this diploma thesis, making this important point for long-term stability.

This is to ensure the up-to-date security level in organization and security level of critical data and information according to latest needs.

3.2.6. Financial burden of security measures

Prices for above listed actions differs based on the extent of the risk analysis, personal audit and afterwards the number of computer where the software tools are implemented. In assumption that organization meets basic criteria in hardware background like servers, not out dated computers, internal networks setup etc., prices begins on approximately 500 000 US dollars up to a 4 US million dollars, which is for medium sized government of South Africa size maximum price. Companies offering their services, software tools and other means intended for cyber security are also offering partnership services after purchases, meaning that costs in further years can be expected but at reasonably lower prices, moving around one-fourth to one-sixth from initial price making services and tools of the company sustainable and accessible in long-term run. Exact price offers for potential costumers of such extent are always opened for price negotiation and based on company’s experiences in implementing security measures in governmental field, prices might drop lower thanks to knowledge base and broader idea what can be expected in such organization, it’s structure, processes and so forth. Broader estimation cannot be however precisely expelled without any information from subject side.

Conclusion

Africa as a continent always had a great potential thanks to it's natural endowments, position, neigbouring continents, access to sea, opportunities relying in building trade partners, however is facing last decades a challenges in promoting development and ensuring basic living standards for it's own citizens. Now days in 21st century besides long-lasting issues in basic living conditions, social disparities, infrastructure issues and many others African Union Member States faces a global challenge of different kind that has evolved in recent years due to the great boom and upsurge of information technology devices and the area, that is today recognized and perceived as cyber environment beneath which are awaiting new threats.

However all those threats hidden in the cyber environment vary thanks to devousiness, accessible technical information, decreasing entry level with technical and knowledge requirements on malicious attackers. Techniques that organization has to be aware of in today's world are expanding from traditional exterior attacks towards the organization to attacks that involve so called social engineering – abusing individual's authorized access for own benefit, uncouncious steps and missclicks of users due to demanding technical environment, unintended access to sensitive information etc., which together represent a new group and branch in cyber security that organization has to focus on.

Networking and computerizing in organizations is inevitable step that is already in second decade of 21st century applied and widely used across different organizations in the world where is expected even great number of users, devices and organizations involved in digital world. Such great increase in usage of network-connected devices used for various tasks as personal data processing, medium for storing information, patents, knowledge, processes etc. requires on organizations to undertake necessary steps to ensure besides fluent functioning and accessible services also necessary security measures to achieve basic level of security standards in today's world and to obey state and international laws. As it was pointed in case studies which focused on trend of attacks, type of attackers, targets, information that attackers desire for and more importantly, financial burden to organization/state budget that accounts for increasing portion of financial menas that could be invested and more effectively used for regional development of the region. On top of that was suggested to extend the coverage of encryption of information to other sectors are parts of government as it is the easiest, most effective and the cheapest way of locking down the content of data to unauthorized persons, either to outsiders or insiders.

As it was futher analyzed in this diploma thesis, approach of governments, unions, international organizations and private enterprises towards cyber security have emerged in recent few years and African Union is one of examples. Thanks to the African Union Convention on Cyber Security and Personal Data Protection, Africa has built up sufficient necessary legislative background and ensured support on governmental level to undertake preliminary steps for implementation of cyber security measures across state organizations to be able to compete on global environment where the increasing proximity and number of attacks can be expected. Security standards have always been perceived by potential partners, states and other subjects interested in cooperation as an obligation. In this century such security standards have already appeared in cyber world to ensure certain level of security standards for successful establishmenet of partnerships.

Objective of this diploma thesis was to analyze situation and environment in African Union on legislative level with practical insights of current trends and costs from various sources to make a complementary review of cyber security dilemma in Africa. On top of that, suggestion part goal was to propose a potential guide to follow and implement an Information Security Information Management that will predominantly ensure information security through data encryption in case of loss or alienation of the information with no possible way to abuse such information assets in favor of the third party. Such measures and tools implemented will facilitate financial burden to state budget thanks to preservation of the content of abused information falling under the provision of Convention on Cyber Security and Personal Data Protection which will positively reflect in regional developemnt of the state. Information security will also have a positive impact on regional and global level, leaving secured information from 3rd parties for disclosure of content of the information that would give them advantages in future dealing with state bodies.

Question of security is gradually evolving area based on the time and space which needs to be followed in advance according to technologies used by different subjects in various environments. Specific area of Cyber Security is a matter that is for the moment at very start for Member States of African Union, leaving this topic open for a necessary initial step by any Member State to deal with this matter, undertake first steps towards cyber security and spreading their experiences, notes and support across public, private sector and possibly in the future, across whole African Union.

References

[1] *AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION* [online]. Malabo: Assembly of the African Union, 2014 [cit. 2016-05-06]. Avaliable from: http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf

[2] Budget Review. *National Treasury Republic of South Africa* [online]. 2015 [cit. 2016-05-14]. Avaliable from: http://www.treasury.gov.za/documents/national%20budget/2015/review/FullReview.pdf

[3] Business process re-engineering. *The Economist* [online]. 2009 [cit. 2016-05-16]. Avaliable from: http://www.economist.com/node/13130298

[4] CAPELLO, Roberta. *Location, Regional Growth and Local Development Theories* [online]. 2012 [cit. 2016-05-16]. Avaliable from: www.fupress.net/index.php/ceset/article/download/9559/8912

[5] Car Theft and Hijackings South Africa. *Bloomberg* [online]. 2014 [cit. 2016-05-14]. Avaliable from: http://www.bloomberg.com/news/articles/2014-10-13/car-theft-and-hijackings-cost-south-africa-770-million-in-2013

[6] *Consultancy: IBM: Retail top target sector for cyber attacks in 2014* [online]. 2015 [cit. 2016-05-06]. Avaliable from: http://www.consultancy.uk/news/1349/ibm-retail-top-target-sector-for-cyberattacks-in-2014

[7] CRESSMAN, Darryl. *Simon Fraser University: A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation* [online]. Simon Fraser University, 2009 [cit. 2016-05-06]. Avaliable from: http://blogs.sfu.ca/departments/cprost/wp-content/uploads/2012/08/0901.pdf

[8] Cyber incidents against government agencies. *Law Enforcement Cyber Center* [online]. 2016 [cit. 2016-05-16]. Avaliable from: http://www.iacpcybercenter.org/cyber-incidents-against-government-agencies/

[9] DAWNKINS, Casey J. *Regional Development Theory: Conceptual Foundations, Classic Works, and Recent Developments*[online]. Sage Publications, 2003 [cit. 2016-05-06]. Avaliable from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.197.6878&rep=rep1&type=pdf

[10] DRAFT AFRICAN UNION CONVENTION ON THE CONFIDENCE AND SECURITY IN CYBERSPACE. *NATO Cooperative Cyber Defence Centre of Excellence* [online]. 2012 [cit. 2016-05-11]. Avaliable from: https://ccdcoe.org/sites/default/files/documents/AU-120901-DraftCSConvention.pdf

[11] *EY: Cyber threat intelligence − how to get ahead of cybercrime* [online]. 2014 [cit. 2016-05-06]. Avaliable from: http://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf

[12] *Gemalto: 2015, The Year Data Breaches Got Personal* [online]. 2016, **2015** [cit. 2016-05-06]. Avaliable from: http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf

[13] Global CYBERSECURITY INDEX & CYBERWELLNESS PROFILES. *The International Telecommunication Union* [online]. 2015 [cit. 2016-05-14]. Avaliable from: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

[14] Hackmageddon. *Hackmageddon: Cyber attacks statistics* [online]. 2015 [cit. 2016-05-06]. Avaliable from: http://www.hackmageddon.com/2012/06/21/june-2012-cyber-attacks-statistics-part-i/

[15] HANSEN, Lene a Helen NISSENBAUM. *International Studies Quarterly: Digital Disaster, Cyber Security, and the Copenhagen School* [online]. 2009 [cit. 2016-05-06]. Avaliable from: https://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf

[16] *HTXT Africa: POLICE DATABASE HACK TOPS LIST OF SA SECURITY BREACHES* [online]. 2015 [cit. 2016-05-06]. Avaliable from: http://www.htxt.co.za/2015/09/09/police-database-hack-tops-list-of-sa-security-breaches/

[17] *Channel New Asia: Singapore one of 5 countries in region most vulnerable to cyber attacks* [online]. 2016 [cit. 2016-05-06]. Avaliable from: http://www.channelnewsasia.com/news/singapore/singapore-one-of-5/2541456.html

[18] *IKANOW: Cyber Threat Intelligence Platform: What are the threats not implementing one?* [online]. 2014 [cit. 2016-05-06]. Avaliable from: http://www.ikanow.com/cyber-threat-intelligence-platform/

[19] NATO Cooperative Cyber Defense KLIMBURG, Alexander. : National Cyber Security Framework Manual [online]. Talinn: NATO CCD COE Publication, 2012 [cit. 2016-05-06]. Avaliable from: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

[20] *Kybez: Základní názvosloví* [online]. [cit. 2016-05-07]. Avaliable from: https://www.kybez.cz/bezpecnost/zkb

[21] LATOUR, Bruno. *: REASSEMBLING THE SOCIAL* [online]. Oxford: Oxford University Press, 2014 [cit. 2016-05-06]. ISSN ISBN 0-19-925604-7 978-0-19-925604-4. Avaliable from: http://www.ufrgs.br/ppgas/portal/arquivos/orientacoes/LATOUR_Bruno._2012.pdf

[22] MOAZ, Zeev, Lesley G. TERRIS, Ranan D. KUPERMAN a Ilan TALMUD. *International Relations: A Network Approach* [online]. 2003 [cit. 2016-05-06]. Avaliable from: http://soc.haifa.ac.il/~talmud/pdf/irnetworks1.pdf

[23] MULLIGAN, Helen a Owen O'RORKE. *Bloomberg: World Data Protection Report*, The Growing Threat of Cyber Attacks in Africa [online]. London, 2015, **2014**(7) [cit. 2016-05-06]. Avaliable from: http://www.farrer.co.uk/Global/Briefings/Bloomberg%20BNA%20World%20Data%20Protection%20Report.pdf

[24] National Cybersecurity Policy Framework for South Africa. *Cyanre South Africa* [online]. 2011 [cit. 2016-05-14]. Avaliable from: http://www.cyanre.co.za/national-cybersecurity-policy.pdf

[25] Net Losses: Estimating the Global Cost of Cybercrime. *MacAfee* [online]. 2014 [cit. 2016-05-14]. Avaliable from: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[26] *Notice of Intention to make South Africa National Cybersecurity Policy* [online]. 2010 [cit. 2016-05-14]. Avaliable from: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/docs/100219cybersecurity.pdf

[27] PASSOTH, Jan H. a Nicholas J. ROWLAND. *Acting in International Relations? Political Agency in State Theory and ActorNetworks*[online]. [cit. 2016-05-06]. Avaliable from: https://millenniumjournal.files.wordpress.com/2012/10/lse-conf-paper-passoth-rowland-2012.pdf

[28] SIMON, Kai A. *: Towards a theoretical framework for Business Process Reengineering* [online]. Göteborg: Göteborg University, 1994 [cit. 2016-05-06]. Avaliable from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.115.6439&rep=rep1&type=pdf

[29] *Soltra: Threat context SOLTRA | AN FS-ISAC DTCC COMPANY CYBER SECURITY PANEL* [online]. 2015 [cit. 2016-05-06]. Avaliable from: http://slideplayer.com/slide/8390853/

[30] South Africa GDP. *Trading Economics* [online]. 2016 [cit. 2016-05-14]. Avaliable from: http://www.tradingeconomics.com/south-africa/gdp

[31] SZAJNOWSKA-WYSOCKA, ALICJA. *THEORIES OF REGIONAL AND LOCAL DEVELOPMENT – ABRIDGED REVIEW* [online]. University of Silesia, Poland, 2009 [cit. 2016-05-06]. Avaliable from: http://webcluster.biol.uni.torun.pl/geo_stary/www/bulletin/12_2009/05_szajnowska.pdf

[32] Tax evasion costs South Africa 'billions'. *African Business Review* [online]. 2012 [cit. 2016-05-15]. Avaliable from: http://www.africanbusinessreview.co.za/finance/1066/Tax-evasion-costs-South-Africa-billions

[33] The cost of cyber-crime in South Africa. *BusinessTech* [online]. 2014 [cit. 2016-05-15]. Avaliable from: http://businesstech.co.za/news/internet/60021/the-cost-of-cyber-crime-in-south-africa/

[34] World's Biggest Data Breaches. *Information is beautiful* [online]. 2016 [cit. 2016-05-06]. Avaliable from: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/