2012/3

The South African Cyber Threat Barometer

A strategic public-private partnership (PPP) initiative to combat cybercrime in SA.

Researched by:

WOLF PACK

Sponsored by:

British High Commission Pretoria

Foreword

Africa is considered to be the cradle of mankind. There is evidence that some of the earliest people lived in southern Africa.

The hunter-gatherer San roamed widely over the area and the pastoral KhoiKhoi wandered in the well-watered parts where grazing was available. Tribes from central Africa moved southwards into the eastern and central parts of the area known today as South Africa.

Milestones in South African history:
1652 – Dutch Settlers arrive under the leadership of Jan van Riebeeck
1795 – British occupation of the Cape
1800 onwards – the Zulu kingdom under King Shaka rises to power
1835 – The Great Trek – Dutch and other settlers leave the Cape colony
1879 – Anglo-Zulu War
1880 – First Anglo-Boer War
1899 – Second Anglo-Boer War
1912 – The African National Congress (ANC) is founded
1961 – South Africa becomes a republic
1990 – Mandela is freed after 27 years in prison and opposition groups are unbanned
1994 – South Africa's first democratic election

South Africa has journeyed through many great obstacles to become a nation whose dream of unity and common purpose is within grasp of all its people. We must not lose sight of this dream. As proud stakeholders of this great country we are now called upon to join hands in the fight against a new threat that is targeting all areas of our society – no organisation, community or child is immune to its impact.

Craig Rosewarne
Managing Director
Wolfpack Information Risk (Pty) Ltd

I am referring to the scourge of cybercriminal activity that is rapidly becoming a global concern and one that we as Africans need to prioritise. We hope this project and proposed initiatives will go a long way towards "rallying the troops" to urgently address the growing cyber threat facing our country.

I wish to offer my sincere appreciation to the British High Commission for their funding and support to complete this vital research project.

I also wish to convey my warmest thanks to all participating companies and teams for their input and independent review of this report. Your passion to make a positive impact in this country has been amazing to witness.

I would finally like to acknowledge the Wolfpack team for their dedication shown in the research, analysis, layout and distribution of this report. I am very proud of what we have achieved.

Corporate contact details:

Building 1 Prism Office Park
Ruby Close, Fourways
Johannesburg, 2055
Telephone: +27 11 367 0613
Email: info@wolfpackrisk.com
Website: www.wolfpackrisk.com

Table of Contents

Foreword 1
British High Commission Pretoria 3
Introduction 4
Executive Summary 5
International Cyber Security Models 9
Global Drivers for Cybercrime 12
International Cyber Initiatives 13
Examples of Recent Cyber Incidents 17
African Perspective 24
South African Perspective 34
National Cyber Security Framework 38
Malware Analysis 42
SA Cyber Security Academy 49
Cybercrime Section 52
A Framework for Analysing the Costs of Cybercrime 56
Conclusion 69
References 70

British
High Commission
Pretoria

Her Excellency Dame Nicola Brewer
British High Commissioner to
South Africa, Swaziland and Lesotho

The growth of the internet has transformed our everyday lives. My day used to start with the newspapers and overnight diplomatic telegrams. Now the first thing I tend to look at is Twitter.

But with greater openness, interconnection and dependency comes greater vulnerability. The threat to our national security from cyber attacks is real and growing. Organised criminals, terrorists, hostile states, and 'hacktivists' are all seeking to exploit cyber space to their own ends. South Africa is no exception – which is why the UK is keen to work closely with both the South African government and the private sector to tackle this together.

The UK Government has moved swiftly to tackle the growing danger posed by cyber attacks. Our National Security Strategy in 2010 classed cyber security as one of our top priorities alongside international terrorism, international military crises and natural disasters. To support the implementation of our objectives we have committed new funding of £650m over four years for a transformative National Cyber Security Programme to strengthen the UK's cyber capabilities. In November 2011 the UK Government published a Cyber Security Strategy (available online), setting out how the UK will tackle cyber threats to promote economic growth and to protect our nation's security and our way of life.

One of our key aims is to make the UK one of the most secure places in the world to do business. Currently, around 6 per cent of the UK's GDP is enabled by the internet and this is set to grow. But with this opportunity comes greater threats. Online crime including intellectual property theft costs the UK economy billions each year. Governments cannot tackle this challenge alone. The private sector – which owns, maintains and creates most of the very spaces we are seeking to defend – has a crucial role to play too. Our Cyber Security Strategy aims to build a real and meaningful partnership between Government and private sector in the fight against cyber attacks, to help improve security, build our reputation as a safe place to do business online, and turn threats into opportunities by fostering a strong UK market in cyber security solutions.

Cyber risks are transnational in nature. We are working with other countries to tackle them. Through the London Cyber Conference, hosted by the UK Foreign Secretary in late 2011, the UK is taking a lead in addressing international discussions on how we can establish a more focused international dialogue to develop principles to guide the behaviour of Governments and others in cyberspace. We will continue to foster this level of international dialogue through various fora including next month's Budapest Cyber Conference, and through international cooperation on tackling cyber crime.

I am delighted that the British High Commission in South Africa has funded the production of this 'Cyber Threat Barometer for South Africa'. I am confident it will help identify and clarify some of the main threats facing South Africa, as well as providing areas for the UK and South Africa to work together to advance the security and prosperity of both countries.

1 Introduction

A scalpel in the right hands can save lives. In the wrong hands it can cause serious damage.

Information is no different. Today it is the lifeblood that connects people, organisations and nations around the globe. Increasingly information traverses within cyber arteries powered by information and communication technologies (ICTs).

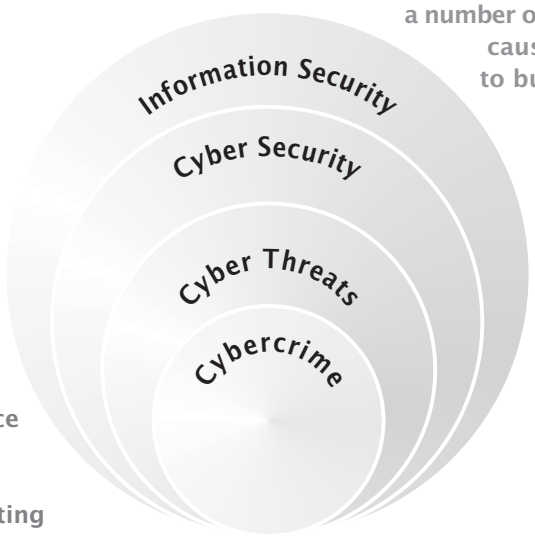
With the rise of the Internet as a platform to share information and conduct business online, the world has never been as connected as it is today. Unfortunately the threat to the confidentiality, integrity and availability of information is also increasing at a similar rate. Cyber attackers, hacktivists, criminal elements and nation states are today using the internet to:-

- Deny and/or disrupt access to information
- Destroy information
- Steal information
- Manipulate information
- Alter the context in which the information is viewed
- Change the perceptions of people towards the information

Cyber attackers exploit numerous vulnerabilities in cyberspace to commit these acts. The increasing complexity and nature of these threats is becoming increasingly difficult to manage.

Information Security - The "CIA Model" - 3 aspects of information (and information infrastructure services) that need to be maintained: Confidentiality, Integrity and Availability.

Cyber Security - the globally interconnected information infrastructure that includes the internet, telecommunications networks, computer systems and industrial control systems. It is increasingly being used for a number of criminal activities (cybercrimes) causing significant financial losses to businesses and individuals alike.



Cybercrime refers to unauthorised access to, interception of or interference with data, computer-related extortion, fraud and forgery, attempt, and aiding and abetting cybercrime. (ECT Act, 2002)

Cyber Threats include any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application or a computer system using the Internet, without lawful authority.

Cyber Threats include

- Cybercrime,
- Cyber Espionage,
- Cyber Terrorism and
- Cyber Warfare.

The focus of this research report is on cyber security with an emphasis on cybercrime and minimal coverage of cyber espionage, terrorism or warfare.

2 Executive Summary

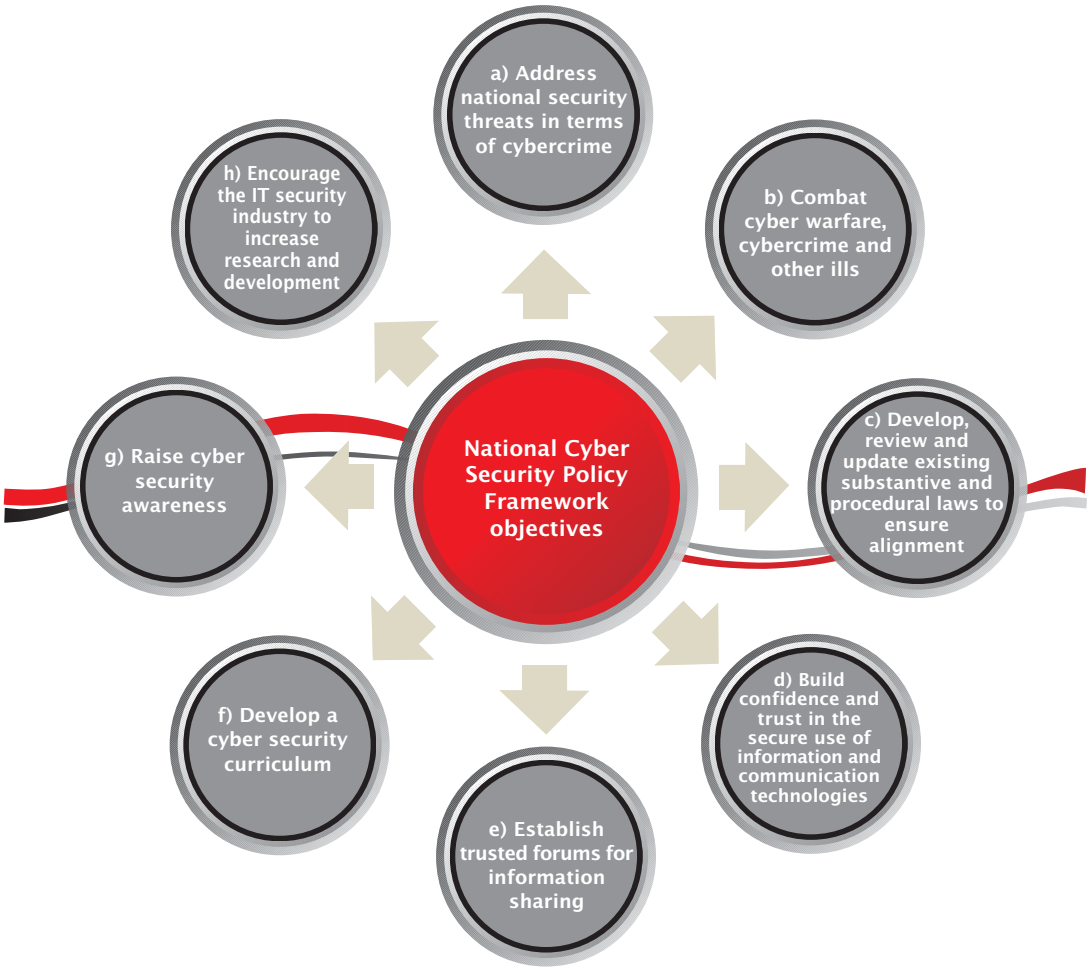
PURPOSE

The intention of the 2012 SA Cyber Threat Barometer research report is to provide ongoing strategic insight and opinion in support of Cabinet's recently approved National Cyber Security Policy Framework for South Africa.

The 2012 SA Cyber Threat Barometer is a strategic public-private partnership (PPP) research project conducted by the Wolfpack Information Risk research team with external funding from the British High Commission. This research project is supported by the SA Chamber of Commerce and Industry (SACCI) and the Information Security Group of Africa (ISGA) who both wish to improve the consistency and efficiency in addressing information security threats facing their respective stakeholder communities.

INTRODUCTION

In March 2012 Cabinet approved the National Cyber Security Policy Framework for South Africa. In summary, this framework outlines policy positions that are intended to:



The policy framework will see a number of structures and institutions established for co-ordinating the work of various security cluster departments that are working on a wide range of issues.

The policy framework identifies specific areas of responsibility by a number of government departments and the State Security Agency is tasked with overall responsibility and accountability for coordination, development and implementation of cyber security measures in the country, as an integral part of its mandate.

The Justice, Crime Prevention and Security (JCPS) Cluster will deal with the details of this policy framework at future briefing sessions.

Project Stakeholders

The intention of this project was to collaborate with key local and international stakeholders to help raise awareness of cyber threats at a strategic level, forge relationships across all sectors and to help fast-track research into the selection of the best cyber threat countermeasures.

To encourage accurate input into this report we provided an assurance of anonymity to all stakeholders that participated in the interview workshops or who reviewed the report at various stages. The following review process was followed:

1. Draft report submitted to individual participants to review their input for accuracy
2. Final draft report ⟶ submitted to steering committee and subject matter experts for review
3. Final report generated

We will furthermore endeavour to establish task teams to manage ongoing proposed cyber security initiatives to ensure all collaboration efforts are sustained.

Structure of Research Report

1 International analysis

- Investigate global drivers for the increase in cyber threats and cybercrime
- Review international cyber security initiatives
- Review international cyber threat models used in countries such as the United States of America, Great Britain, Brazil, Russia, India and China (BRIC) countries
- Review international cyber security initiatives, laws and stakeholders
- Analysis of recent international cyber incidents over a 6 month period

2 Africa analysis

- Analysis of African internet penetration
- Review African cyber security initiatives
- Review of laws and key stakeholders for selected African countries

3 Analysis of Malware from International Security Providers

- Review and analysis of local malware statistics for South Africa

4 South Africa analysis

- South African international cooperation initiatives
- Interviews with key stakeholders from the South African government, banking and telecommunications sectors.
- Valuable input was furthermore received from international stakeholders, universities, industry bodies and information security / cyber forensics specialists.

5 Summary of key issues identified

In our analysis of the data collected from interviews conducted with local and international stakeholders, a number of common issues were identified, which we have categorised below:

Key issues identified	Category
Denial of service, economic fraud and the theft of confidential information were cited as the main concerns for SA. The top cyber services targeted are internet banking, ecommerce sites and social media sites. Criminals are typically mainly after logon credentials, bank or credit card information and personally identifiable information. The most common attack methods are still phishing, the abuse of system privileges and malicious code infections. The common top cyber vulnerabilities are: • Inadequate maintenance, monitoring & analysis of security audit logs • Weak application software security • Poor control of admin privileges • Inadequate account monitoring & control • Inadequate hardware/software configurations The internal monitoring of suspicious transactions and the general use of internal and 3rd party fraud detection mechanisms are still the most effective means of detecting cybercrime.	Threat & vulnerability management
More collaboration on public / private initiatives is needed. The banking sector in partnership with SABRIC were seen to be the leading industry when it came to establishing working public-private partnerships for the prevention and combating of cybercrime. Government alone cannot combat crime and key partnerships across multiple sectors in SA, the African continent as well as internationally are vital to the country's success going forward.	Collaboration
The lack of a functional national Computer Security Incident Response Team (CSIRT) in South Africa was identified as a major concern. A National awareness programme addressing major risks facing SA should be implemented. It was felt that if the government does not create an effective CSIRT soon that private industry would have to consider establishing their own industry-specific centres and ultimately a private national operation. This has already begun in the financial sector.	Government initiative
A national baseline information security qualification or curriculum is required for SA. It is furthermore valuable to consider the concept of a national cyber security academy. It was acknowledged that a shortage of experienced computer forensics, incident handlers and secure software coding skills are in short supply. Deeper investments into training and skills development across all sectors is needed with a focus on deeper investigative and prosecutorial skills. We need to selectively train relevant police constables basic cybercrime skills on how to identify, categorise and open a docket for cybercrime incidents.	Skills development
Deeper research is required on actual threats facing South Africa and selected African countries.	Research

Key issues identified	Category
Occurrences of cybercrime are on the increase across all three sectors interviewed. The estimated price tag of cybercrime to the sectors within scope of the research was R2.65 billion with an average recovery rate of 75% resulting in the actual loss figure estimated at R662,5 million. It was agreed that on average most perpetrators still exploit common vulnerabilities using often repeated attack methods. The overall process of reporting cybercrime to law enforcement at a station level is highly inefficient. Higher levels of satisfaction were however reached dealing at a commercial branch level especially when based on established relationships. It was felt that individuals or small companies that incur cybercrime losses under a certain financial threshold are very much left to fend for themselves.	Cybercrime
Considering SA's position as a developing country, their regulatory and legislative framework for information security compares well against other developing countries. The implementation however of good practice is still lagging, especially in the small to medium sector space. The ECT act is seldom used to prosecute cybercrimes due to weaker penalties and common law practices are instead being used. Whilst this is good for attaining harsher sentences, cybercrime statistics are as a result diluted with common law crimes such as fraud or theft. The National Prosecuting Authority (NPA) are only exposed to a smaller percentage of cases that are handed over by the police and less than 5% make it to court and are categorised as cybercrime.	Legal framework

6 Proposed initiatives – Going forward

Achieving the vision of keeping our cyberspace a safe place to conduct business and interact will require continued collaboration across government, the private sector and stakeholder communities.

Based on our review of international case studies and interviews with local specialist we have recommend the following initiatives for further consideration and have provided additional detail throughout the report.

Short-term initiatives

- National Cyber Security Framework
- SA Cyber Security Academy
- Cyber Threat Research Programme

Medium-term initiatives

- Establishment of a National CSIRT
- National Awareness Programme

3 International Cyber Security Models

Cyberspace touches nearly every part of our daily lives. It's the broadband networks beneath us, the wireless signals around us, the local networks in our schools, hospitals, businesses and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the world wide web that has made us more interconnected than at any time in human history. We must secure our cyberspace to ensure that we can continue to grow the nation's economy and protect our way of life.

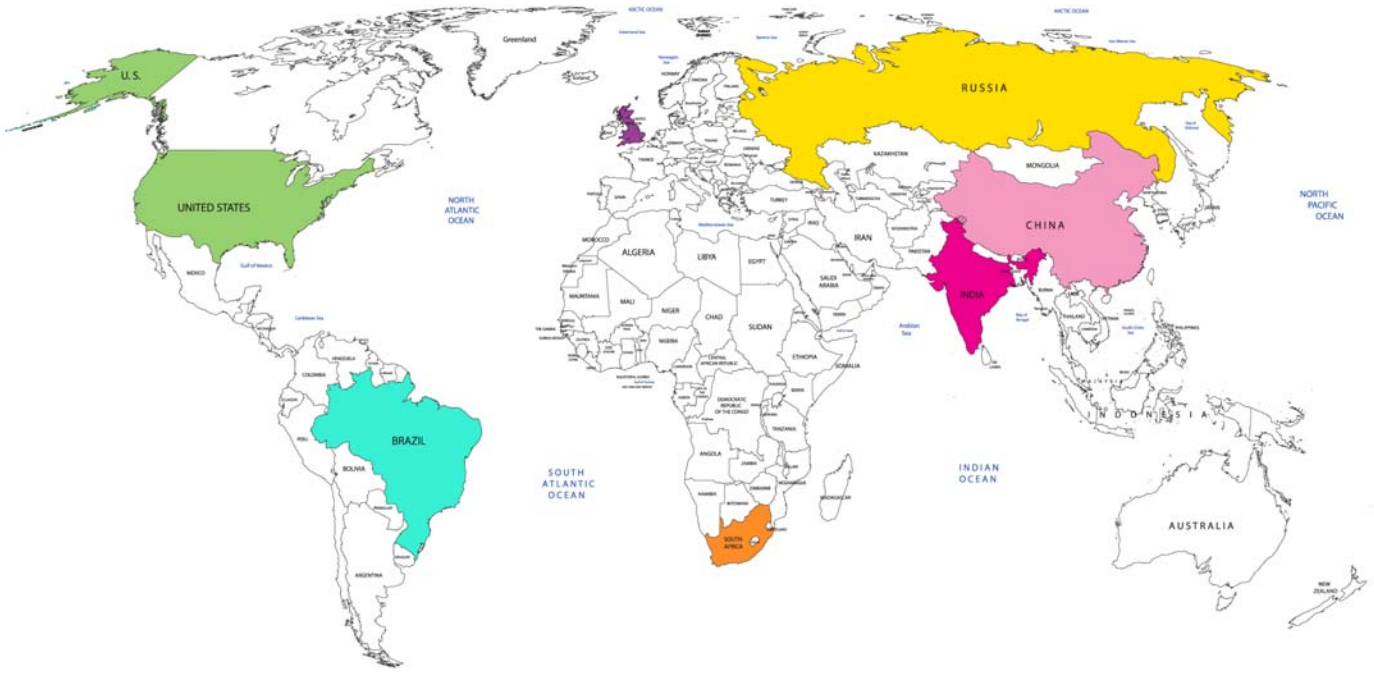
US President Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber security."

In 2010, the UK government announced a £650m investment strategy into cyber security & declared that cyber security had become a 'tier 1' priority alongside international terrorism and major national incidents.

The UK is one of many governments around the world which recognise the serious nature of the threat that is emerging from the cyber-sphere. Nations of the world are giving serious priority to implementing cyber security strategies that will both improve their resilience to cyber incidents and where possible reduce the impact of cyber threats.

As part of our research to provide recommendations to South African stakeholders we reviewed and analysed national cyber security initiatives currently underway within the following countries:-

- United States of America
- United Kingdom
- BRICS Countries – Brazil, Russia, India, China and South Africa



Summary of National Cyber Security and Cybercrime Initiatives
(see separate country reports on www.wolfpackrisk.com for greater detail)

Country	Policy / Acts / Regulations / Guidance	Budapest Convention Signed	Budapest Convention Ratified	CERT / CSIRT	Member of FIRST	Selection of Cyber Security Stakeholders
USA	• Computer Fraud and Abuse Act (CFAA) • Electronic Communications Privacy Act (ECPA) • National Infrastructure Protection Act • Cyberspace Electronic Security Act • Digital Millennium Copyright Act • Patriot Act of 2001 • Cyber Security Enhancement Act (CSEA) • Anti-Phishing Act • Cybersecurity Act of 2010 • Cyber Security and Internet Freedom Act of 2011 • USA Cyber Security Information Sharing Act of 2012 • SECURE IT Act of 2012 • Cyberspace Policy (Draft)	Yes	Yes	• Computer Emergency Readiness Team/Coordination Center (CERT/CC) at Carnegie-Mellon • US- USCERT • Sector specific US CERTs • Energy • NASA • Military • Industrial (ICS-CERT) • SANS Internet Storm Center	Yes	• Department of Defense Cyber Crime Center (DC3) • Defense Cyber Crime Institute (DCCI). • U.S. Immigration and Customs Enforcement Cyber Crimes Center (C3) • The Computer Crime and Intellectual Property Section (CCIPS) • Federal Bureau of Investigation • National Infrastructure Protection Center • National White Collar Crime Center • Internet Fraud Complaint Center • Computer Crime and Intellectual Property Section of the Department of Justice (DoJ) • Central Intelligence Agency (CIA) • National Security Agency (NSA) • Computer Emergency Readiness Team/Coordination Center (CERT/CC) at Carnegie-Mellon
UK	• Data Protection Act 1998 • UK National Cyber Security Strategy of 2011 (to 2015) • Computer Misuse Act 1990 • Privacy and Electronic Regulations (EC Directive) 2003 • Police and Justice Act 2006 • Serious Crime Act 2007 • European Directive of 1995 • Regulation of Investigatory Powers Act 2000 (also update UK book)	Yes	Yes	• UKCERT • GovCertUK **Sector specific UK CERTs** • Academic • Military • Governmental	Yes	• Government Communications Headquarters (GCHQ) • ACPO (Association of Chief Police Officers, ACPO e-crime Committee/ ACPO e-crime strategy) • Action Fraud (UK's national fraud and internet crime reporting centre) • NFIB (The National Fraud Intelligence Bureau) • SOCA (The Serious Organised Crime Agency) • CSOC (The Cyber Security Operations Centre) • Get Safe Online • Home Office • Metropolitan Police Force eCrime Unit • IWF (The Internet Watch Foundation) • OCS (The Office of Cyber Security) • PCeU (The Police Central e-crime Unit) • London Action Plan on Spam Enforcement
BRAZIL	• Brazilian Senate's Substitute Act to the House Bill No.89 of 2003 ("Draft Law") - under review (Article 19) • Criminal Code (Article 28) • Law no. 9,983 of July 7, 2000	No	No	• CERT.br National Government CSIRT • CAIS/RNP	Yes	Brazilian Federal Police Computer Forensic Unit

Country	Policy / Acts / Regulations / Guidance	Budapest Convention Signed /	Ratified	CERT / CSIRT	Member of FIRST	Selection of Cyber Security Stakeholders
RUSSIA	• Russian Federation's Criminal Code	No	No	ruCERT CERT-GIB	Yes	• Group-IB • Russian Security Council • Russian Association of Electronic Communication (RAEC) • The Russia Federal Security Service (FSB) Center for Electronic Surveillance of Communications (TSRRSS) • Federal State Unitary Enterprises(FGUP) supervised by the Federal Security Service (FSB) • FGUP STC Atlas • FGUP Center-Inform • Russian firm OOO Speech Technology Company (STC) • Kaspersky Labs
INDIA	• Information Technology Act, 2000 • Indian Penal Code • Indian Evidence Act • Bankers' Book Evidence Act • Code of Criminal Procedure, Civil Procedure Code • Reserve Bank of India Act	No	No	CERT-In	Yes	• Inter Departmental Information Security Task Force (ISTF) • National Security Council • National Critical Information Infrastructure Protection Centre (NCIPC) • Defence Intelligence Agency (DIA) • National Technical Research Organisation (NTRO) • NASSCOM • Information Security Council of India (DSCI) • National Informatics Centre (NIC)
CHINA	• 7th Amendment of China Penal Code (Article 312) • Criminal Law of the People's Republic of China (Article 285, 286, 287) • Decision on Protecting Security of Network • Telecommunication Ordinance • Guarding State Secrets Law • Jurisdiction and International Cooperation • Criminal Procedure Law	No	No	• CCERT • CMCERT/CC • CNCERT/CC • HKCERT • HUAWEI NSIRT	Yes	• Public Security Bureau (PSB) • CAST (China Anti-Spam Team) • ASEAN, China Coordination Framework for Network and Information Security Emergency Responses • APEC Working Group on Telecommunications
SOUTH AFRICA	• Criminal Code or Statute – Prevention of Organised Crime Act, 1998, Prevention of Organised Crime Amendment Act, 1999, Prevention of Organised Crime Second Amendment Act, 1999 • Criminal Procedural Code or Statute – Criminal Procedure Act, 1977, Proceeds of Crime Act, 1996 • Extradition Law – Extradition Amendment Act, 1996, Banking, Securities & Financial Law, Financial Intelligence Centre Act, 2008, • Anti-corruption Law – Prevention and Combating of Corrupt Activities Act, 2004 • Police and Law enforcement Law – South African Police Service Act, 1995, Special Investigating Units and Special Tribunals Amendment Act, 2001, Special Investigating Units and Special Tribunals Act, 1996 • MLA Law – International Co-operation in Criminal Matters Act, 1996 • Constitutional and Administrative Law – National Prosecuting Authority Amendment Act, 2000, National Prosecuting Authority Act, 1998, Constitution of the Republic of South Africa, 1996 • Investigation of Serious Economic Offences Amendment Act, 1995, South Africa More specific to Information / Cyber Security • The Electronic Communications and Transmissions Act (ECT, 2002) • The Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA, 2002) • Protection of Personal Information Bill (POPI, 2009) • Electronic Communications Security Pty (Ltd) Act (ECS, 2002) • King Code of Governance for South Africa 2009 (KING III) • National Cybersecurity Policy Framework • MIS Act • State Information Technology Agency Act (Act 88 of 1998)	Yes	No	• No National CSIRT is established as yet • CSIRTFNB Computer Security Incident Response Team (First National Bank) • E-COMSEC (SA Government only)	Yes	**Justice, Crime Prevention and Security (JCPS)** • South African Police Service (SAPS) • Directorate for Priority Crime Investigation (HAWKS) • State Security Agency (SSA) • Department of Communications • Department of Defence and Military Veterans • Department of Home Affairs • National Prosecuting Authority (NPA) • Special Investigating Unit (SIU) • Department of Justice and Constitutional Development • Department of Science and Technology • Independent Communications Authority of SA • SA Banking Risk Information Centre (SABRIC) • Council for Scientific and Industrial Research (CSIR) • Southern African Fraud Prevention Service (SAFPS) • The SA Cyber Security Academic Alliance • Information Security Group of Africa (ISG Africa) • e-Commerce Advisory Committee (ECAC), • Information Security SA (ISSA) • ITWeb Security Summit

4 Global Drivers for Cybercrime

The rise of cybercrime in the last decade is an economic case of individuals responding to monetary and psychological incentives.

Two main drivers for cybercrime can be identified:

- The potential gains from cyber attacks are increasing with the increased use of the internet for financial, social, political and business transactions, and
- Cyber criminals expected consequences (e.g. the penalties and the likelihood of being apprehended and prosecuted) are frequently lower compared with traditional crimes.

Potential cyber threat categories:

1) Script kiddies
2) Insiders
3) Hacker groups
4) Scammers / Phishers
5) Political/Religious/Hacktivist groups
6) Organised crime syndicates
7) Advanced State sponsored groups

Crimes committed using ICT and especially the internet are more convenient, more inexpensive and therefore more profitable with a lower risk profile than crimes committed using more traditional means.
The increase in cybercriminal activities, coupled with ineffective legislation and ineffective law enforcement pose critical challenges for maintaining the trust and security of global computer infrastructures.

Cybercrime can be summed up as crime that occurs in cyberspace. The field may also be referred to as "computer crime", "internet crime", "high tech crime", or a variety of other related names.
Essentially, we use the term anytime a computer or related technology is used or is in some way involved in a crime. Sometimes it simply contains evidence of a crime. Other times it was used to commit the crime. And in other cases the device essentially is the "victim".

Here is a general (non-comprehensive) list of criminal activity that may fit into this category:

- Production, distribution and downloading of child abuse material
- Copyright infringement, software piracy, trademark violations
- Online harassment
- Distributed denial of service attacks / Botnets
- Hacking
- Advance-fee fraud conducted over the internet
- Identity theft and identity fraud
- Scams and online frauds
- Phishing
- Malicious software and spam
- Attacks against critical infrastructures
- Virtual world or gaming incidents

5 International Cyber Initiatives

Political or natural boundaries are not an obstacle to conducting cybercrime, hence global agreements and initiatives are essential to ensure efficient international co-operation.

Council of Europe Convention on Cybercrime (COECC)

The Council of Europe (COE) established the Budapest Convention of Cybercrime (standards: CETS 185) recognised today as an important international instrument in the fight against cybercrime. The main capacity building project and driver of the COE's action against cybercrime has been the Global Project on Cybercrime. The Convention on Cybercrime distinguishes between four different types of offences:

- Offences against the confidentiality, integrity and availability of computer information/systems;
- Computer-related offences;
- Content-related offences; and
- Copyright-related offences.

The Budapest Convention on Cyber Crime

The Budapest Convention on Cyber Crime was one of the first international community efforts to establish a universal treaty on cybercrime. It is the first international treaty seeking to address computer and internet crimes by harmonising national laws, improving investigative techniques and increasing cooperation among nations. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004.

The objectives of the Budapest Convention include:-

- Stronger and more harmonised cybercrime legislation worldwide;
- Consistent approach to criminalising conduct, procedural powers for law enforcement and international cooperation;
- More efficient international cooperation;
- More investigation, prosecution and adjudication of cybercrime;
- A contribution to human rights and the rule of law in cyberspace

Under the convention, member states are obliged to criminalise:

1. Illegal access to a computer system,
2. Illegal interception of information to a computer system,
3. Interfering with computer system without right, intentional interference with computer information without right,
4. The use of inauthentic information with intent to put it across as authentic (information forgery),
5. Infringement of copyright related rights online,
6. Interference with information or functioning of computer system,
7. Child pornography related offences

Status of signatures and ratifications of the Convention on Cybercrime (Status as of 19/09/2012)

Ratified (32)	Signed (10)	Not signed	Invited to accede (8)
Albania	Czech Republic	Andorra	Argentina
Armenia	Greece	Monaco	Australia
Austria	Ireland	Russian Federation	Chile
Azerbaijan	Lichtenstein	San Marino	Costa Rica
Belgium	Luxembourg		Dominican Republic
Bosnia and Herzegovina	Poland		Mexico
Bulgaria	Sweden		Philippines
Croatia	Turkey		Senegal
Cyprus	Canada		
Denmark	South Africa		
Estonia			
Finland			
France			
Georgia			
Germany			
Hungary			
Iceland			
Italy			
Japan			
Latvia			
Lahuania			
Malta			
Moldova			
Montenegro			
Netherlands			
Norway			
Portugal			
Romania			
Serbia			
Slovakia			
Slovenia			
Spain			
Switzerland			
The former Yugoslav Republic of Macedonia			
United States of America			

Nations supporting this Convention agree to have criminal laws within their own nation to address cybercrime, such as hacking, spreading viruses or worms, and similar unauthorised access to, interference with, or damage to computer systems. Each country should have a single point of contact for international cooperation in cybercrime investigations.

South Africa and many other countries signed the COECC Convention on Cybercrime as a multilateral instrument to address the problems posed by criminal activity on computer networks. However, many states still have to sign let alone ratify the Convention to serve as a deterrent. South Africa has signed the Convention, but has to date not ratified it. The unanimous participation of all nations is thus required to achieve meaningful collaboration.

Multi-Lateral cybercrime initiatives

A number of international organisations work constantly to promote or use collective defenses to analyse the latest developments in cyber threats and cybercrime. Some examples include:

Group	Description
Commonwealth Internet Governance Forum (CIGF)	• This initiative will assist developing Commonwealth Countries to build their institutional, human and technical capacities with respect to policy, legislation, investigation and law enforcement with the aim of making their jurisdictions more secure by denying safe havens to cyber criminals, and assisting member states to be more effective partners in the global effort to combat cybercrime • This will promote the sharing of expertise and best practice from existent resources, focusing upon the Commonwealth Model Law on Computer and Computer related Crime (Model Law) and also drawing from other existent treaties, toolkits, resources and instruments to enable countries to address the legislative gaps so that they can deal with incidents of cybercrime
Council of Europe	• CyberCrime@IPA – joint project of the Council of Europe and the European Union on regional cooperation against cybercrime in eight countries of South-Eastern Europe • European Union Cybercrime Task Force (EUCTF) which was established in 2010 and gathers the heads of high-tech crime units of the 27 Member States of the European Union. The secretariat of the EUCTF is provided by Europol
ENISA (European Network and Information Security Agency)	• Performed their first pan-European cyber-exercise, which next year is slated to include the United States. Concerned with the growth of botnets, ENISA has also published recommendations on mitigating and preventing the threat of bots • The collaboration of governments and the security community has also begun to garner more attention. A recent example of this cooperation was the takedown of the Coreflood botnet, a joint effort that involved federal agents and ISPs
European Commission	• By 2012, the European Commission is expected to create a network of Computer Emergency Response Teams (CERTs) — that can react in the case of computer-related emergencies including cyber-attacks — with a CERT centre in each EU country • European Cybercrime Centre (EC3)

Europol (European Union Law Enforcement Agency)	• Created the European Cyber Crime Task Force in June 2010
	  • Expert representatives from Europol, Eurojust (the EU judicial cooperation body) and the European Commission
	  • Its cybercrime information base provides the EU members with investigative and analytical support on cybercrime and facilitates cross-border cooperation and information exchange
	  • Internet Crime Reporting – centralised coordination of reports of cybercrime from EU Member State authorities and host technical information and training for law enforcement
	  • Strategic analysis of Internet Facilitated Organised Crime iOCTA
	• Produced the iOCTA – a Threat Assessment on Internet Facilitated Organised Crime which aims to:-
	  • Develop new international strategic and operational partnerships
	  • Partner with the private sector and academic community

Group	Description
Forum for Incident Response and Security Teams (FIRST)	• FIRST is the premier organisation and recognised global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents • FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organisations. • FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large
Global Prosecutors E-Crime Network (GPEN)	• Established by the UK Crown Prosecution Service (CPS) and the International Association of Prosecutors [IAP] • The global network of specialists not only encourages enhanced international cooperation in the e-crime arena; but it enables all jurisdictions to develop a co-ordinated approach for dealing with e-crime that supports effective prosecutions and promotes the principles of the Council of Europe Cybercrime Convention
IMPACT (International Multilateral Partnership Against Cyber Threats)	• The world's largest United Nations-backed cyber security alliance • Functions as the cyber security executing arm of the United Nations (UN) specialised agency for ICT – the International Telecommunication Union (ITU) • Being the first comprehensive public-private partnership against cyber threats, IMPACT is the international platform which brings together governments of the world, industry and academia to enhance the global community's capabilities in dealing with cyber threats • IMPACT is the operational home of ITU's Global Cybersecurity Agenda (GCA) • IMPACT with 144 partner countries is now formally part of the ITU-IMPACT coalition • IMPACT is a politically neutral platform, bringing together governments, academia, industry leaders, international organisations, think tanks and cyber security experts to enhance the global community's capacity to prevent, defend against and respond to cyber threats
International Criminal Police Organisation (Interpol)	• Promote the exchange of information among member countries • Coordinate and assist international operations • Establish a global list of contact officers available around the clock for cybercrime investigations (the list contained 131 contacts at the end of 2011) • Assist member countries in the event of cyber-attacks or cybercrime investigations through investigative and database services
International Telecommunication Union (ITU)	• Specialised agency within the United Nations, plays a leading role in the standardisation and development of telecommunications as well as cyber security issues • Importance of international cooperation in the fight against cybercrime and announced the launch of the ITU Global Cyber Security agenda • Highlights the elaboration of global strategies and frameworks for the development of model cybercrime legislation
North Atlantic Treaty Organization (NATO)	• At the NATO summit in November 2010, the EU, NATO and the USA approved plans for a coordinated approach to tackle cybercrime in member states. Under the approval, by 2013 an EU cyber crime centre will be established to coordinate cooperation between member states. Also by that time, a European information sharing and alert system will facilitate communication between rapid response teams and law enforcement authorities

OAS (Organization of American States)	• A group of experts on cybercrime established in 1999. Their aim is to:-
	  • Identify/Create an entity responsible for cybercrime
	  • Enact legislation
	  • Harmonise cyber-laws to facilitate international cooperation
	  • Determine training needs
	  • Educate the public

Group	Description
Organisation for Economic Co-operation and Development (OECD)	• OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
Project MARS (Microsoft Active Response for Security)	• Works with academic and industry experts and utilises technical and legal efforts in an attempt to defeat botnets. The Waledac botnet was shut down through successful legal action after which Microsoft began working with ISPs and Computer Emergency Response Teams (CERTs) to help customers remove the Waledac infection from their computers
Signal Spam	• A public-private partnership initiated by the government that collects spam reports from users and shares them with law enforcement and civil authorities, as well as major email providers, ISPs, and senders, to help remediate the root cause of spam, which is often a computer compromised by a botnet
The Asia-Pacific Economic Cooperation (APEC)	• APEC Telecommunications and Information Working Group aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing information policies • Adopted the APEC Cyber security Strategy
The Group of Eight (G8)	• Established a "Subcommittee773 on High-tech Crimes" (transnational organised crime) which consists of ten principles and a ten-point action plan to fight high-tech crimes
The United Nations (UN)	• Created a working group dealing with spam, cybercrime and other Internet-related topics emphasising the interest of the UN in participating in ongoing international discussions on cybercrime threats • Declaration was adopted that highlighted the need for harmonisation in the fight against cybercrime

Examples of recent cyber incidents between December 2011 – May 2012 (Source: http://hackmageddon.com)

Date	Author	Target	Description	Attack
Dec 1	SECTORLEAKS404	ACNUR La Agencia de la ONU para los Refugiados	SECTORLEAKS404 hacks a Web Server belonging to ACNUR (United Nations Refugees Agency) and leaks credentials of President Barack Obama.	SQLi
Dec 1	Over-X	KASPERSKY lab	Yet another Security Firm victim of defacement. This time the target is Kaspersky, whose Costa Rica Web Site (www.kaspersky.co.cr) is defaced.	Defacement
Dec 4	Unkown	Радио Эхо Москвы	Two Liberal Russian media outlets and an election watchdog became victim to huge cyber-attacks during Russian elections. Sites belonging to the Ekho Moskvy radio station, online news portal slon.ru and election watchdog, Golos, all went down on December the 4th, at around 5am Central European Time.	DDoS
Dec 6	D35MOND142	GstarCAD	One of the victims of D35M0ND142 is GstarCAD, a leading 2d/3d automated cad software technology developer. The website is hacked and taken offline. The leak contains basic database information and a dump of more than 300 user accounts with encrypted passwords.	SQLi

Date	Author	Target	Description	Attack
Dec 7	Greek Hacking Scene	Coca-Cola	Not even Coca Cola is immune from hackers. A Greek hacker called Greek Hacking Scene (GHS) defaces the official website of the multinational company.	Defacement
Dec 8	Unknown	Gemnet	Websites belonging to a Netherlands-based issuer of digital certificates Gemnet become unavailable following reports hackers penetrated their security and accessed internal databases. The access happened thanks to a PHPMyAdmin page without password.	Unprotected Server Page
Dec 9	Four People	Hundreds of Students	The first multimillion scam of the month: British police arrests six people in connection with a phishing scam that targeted hundreds of students, and is believed to have stolen over a million pounds by illegitimately accessing their bank accounts.	Phishing
Dec 10	Four Romanian Hackers	SUBWAY	The US Department of Justice indicts and arrests four Romanians for credit card fraud perpetrated against 150 Subway restaurants and other retailers concluding a three year investigation. According to DOJ, hacking POS the four got their hands on the credit, gift and debit card data of more than 80,000 customers, stealing several millions between 2008 and 2011.	POS Hacking
Dec 10	Unknown	twitter	Russian hackers flood Twitter with automated hashtags to hamper communication between opposition activists. The pro-government messages with the hashtag #???????????? (Triumfalnaya) were generated by a twitter botnet composed by thousands of Twitter accounts that had little activity before.	Twitter Botnet
Dec 11		Coalition of Law Enforcement and Retail CLEAR A National Association	US Law Enforcement agencies are under attack again. This time the attacker is @exphin1ty and the target is clearusa.org (Coalition of Law Enforcement And Retail). The leak contains nearly 2500 account details and personal messages. The web sites is currently (12/16/2011) offline.	SQLi
Dec 13	Unknown	Three U.S. Key infrastructures	At a cyber security conference, Michael Welch, deputy assistant director of the FBI's cyber division, declare hackers had accessed crucial water and power services in three US Cities. During November similar incidents occurred in Springfield and South Houston's water supply network.	SCADA HACK (No details)
Dec 13			@AntiSecBrTeam, as part as what is called #OpAmazonia hacks and defaces some websites belonging to Brazilian Government.	Defacement
Dec 13	Unknown	Russia Political Forums	Another occurrence of Cyber Activity following the elections in Russia: a couple of Russian forums (Superjedi.ru and Attrition.org) on which political topics are debated, are under DDoS attack.	DDos

Date	Author	Target	Description	Attack
Dec 15	ANONYMOUS	UNITED STATES SENATE	Anonymous leaks detailed information on many of the politicians who allowed National Defense Authorization Act (NDAA) passed through the Senate, with 86 senators voting in favor of bill.	N/A
Dec 16		RESTAURANT DEPOT	Details are unveiled about a breach notification letter sent on Nov. 25 by Restaurant Depot to more than 200,000 customers, notifying them about the theft of sensitive information, including names of cardholders, credit or debit card numbers, card expiration dates and verification codes. Fraudsters are believed to be based in Russia. Forensic investigators determined they were able to obtain magnetic stripe card credentials from September 21 through November 18 via the internet by accessing Restaurant Depot's network.	Magnetic Stripe Card Credentials stolen via Unauthorised Access
Dec 20	Indishell		The Personal cyber war between India and Pakistani hacking crews did not stop on December. This time is the turn of Indishell who performed a huge defacement campaign against websites belonging to Pakistan which affected more than 800 sites.	Defacement
Dec 22	Unknown	7K7K	Another massive breach in China affecting a Game site (7k7k.com) and its 20,000,000 users who have their accounts leaked on the Internet.	SQLi
Dec 25	ANONYMOUS	STRATFOR GLOBAL INTELLIGENCE	Anonymous claims to have stolen more than 4,000 credit card numbers and other personal information belonging to clients (ranging from Apple to U.S. Air Force) of U.S.-based security think tank Stratfor. The goal was to pilfer funds from individuals' accounts to give away as Christmas donations, and as a matter of fact some victims confirmed unauthorised transactions linked to their credit cards.	SQLi
Dec 25	Unknown	Taishin Bank	The China Post reports that information of as many as 20,000 applicants for cash cards issued by Taishin International Bank have been found to be part of a massive leak of information. The information was accessed between 2003 and 2005, but it looks like hackers still have access to data.	N/A
Dec 27	Unknown	天涯社区 www.tianya.cn	The registration details of about 40 million users of tianya.cn, a big Chinese social networking site, were found to have been leaked. The details of leaked users have been published in clear text format.	SQLi
Jan 1	ANONYMOUS	MMA	As part of #OpAmaZonaSave 1.0 Anonymous attacks the Brazilian Ministry of Environment (ambiente.gov.br) and leaks server data and some logins.	N/A
Jan 4	Indishell		Another occurrence of the endless cyberwar between India and Pakistan. The indian hacker crew Indishell defaces 30 websites belonging to Pakistan Government.	Defacement

Date	Author	Target	Description	Attack
Jan 6		Symantec	@YamaTough, a member of hacking group the Lords of Dharmaraja, leaks the source code of Symantec Endpoint Protection Enterprise Suite (SAVCE 10.2 and SEP11), approximately 5 years old. The source code was allegedly obtained from the hacking of Indian Military Servers. Symantec admits that “a segment of its source code used in two of our older enterprise products has been accessed”.	N/A
Jan 6	ANONYMOUS	ArcelorMittal	Anonymous breaches the main website belonging to ArcelorMittal, the largest steel producing company in the world, takes the site offline and leaks a large quantity of information from their databases (5000 names and e-mails).	SQLi XSS
Jan 6		SONY PICTURES	As part as #OpSony, Sony Pictures Website is hacked by @s3rver_exe, Anonnerd and N3m3515, once again in the name of the Anonymous movement and against Sony showing its support for SOPA. In the same operation a fake Facebook account is created simulating a real account hacked.	Account Hacking
Jan 8	LulzReborn	GAME	LulzReborn hacks a game website (game.co.uk) and dumps on pastebin nearly 200 usernames and clear text passwords.	SQLi
Jan 15	Unknown	Zappos.com POWERED by SERVICE	Zappos CEO Tony Hsieh says in a letter that customers' names, e-mail addresses, billing and shipping addresses, phone numbers, the last four digits of their credit card numbers, and their scrambled passwords of the Amazon Owned Company might have been illegally accessed, said in a letter sent to although "critical credit card data and other payment data was not affected or accessed."	N/A
Jan 17	Unknown	Postbank A member of the Post Office group	Sources report of a perfectly planned and coordinated bank robbery of over $6.7 million executed during the first three days of the new year in Johannesburg, targeting South African Postbank – part of the nation's Post Office service.	Unauthorised Access
Jan 21	ANONYMOUS	GDF	Anonymous attacks the websites of Brazil's federal district (hundreds of sites that share the URL df.gov.br) as well as one belonging to Brazilian singer Paula Fernandes to protest the forced closure of Megaupload.com.	DDos
Jan 21	#ANTISEC		In the name of the #Antisec movement, an unknown hacker exposes the IP addresses and other details of 49 SCADA systems, inviting the readers to connect and take screenshots of the internals.	Unauthorised Acces
Jan 22			The wave of the #OpMegaUpload arrives in Brazil: @Havittaja and @theevilc0de take down and deface a huge amount of government web sites. The takedowns and defacements last all month.	DDos
Jan 23	Unknown	RG&E NYSEG	The New York State Public Service Commission announces it will conduct a full and complete investigation into the unauthorised access to customer data announced by New York State Electric & Gas (NYSEG) and Rochester Gas and Electric (RG&E).	Unauthorised Access

Date	Author	Target	Description	Attack
Jan 30	ANONYMOUS	Bradesco	Anonymous Brazil takes down one of the biggest Brazilian Banks, Banco Bradesco SA (bradesco.com.br).	DDoS
Feb 16	Unknown	Central Connecticut State University	Central Connecticut State University officials announce that a security breach in a CCSU Business Office computer exposed the Social Security Numbers of current and former faculty, staff, and student workers to potential misuse. The computer was infected by a "Z-Bot" malware that exposed the Social Security Numbers of 18,275 CCSU individuals to potential risk. No other information, such as name or home address, was exposed.	Z-Bot
Feb 21		lanacion.com	@alsa7rx hacks "La Nacion" (lanacion.com.ar) and dumps 451 usernames, e-mail addresses, passwords, and IP addresses on the Internet.	SQLi
Feb 28	ANONYMOUS	INTERPOL	The Anonymous temporarily force the main website for Interpol (Interpol.in) offline, after the international police group announced it had arrested 25 suspected supporters. The site www.interpol.int was unreachable for 20-30 minutes.	DDoS
Feb 4		NASA	After the dump of January, @d4op releases a list of NASA account and passwords including: 403 emails usernames and clear text passwords.	N/A
Feb 12		NASA	NASA hacked again in less than two weeks. @r00tw0rm hack the NASA servers and release a small part of the Database. They also said they advised NASA of the vulnerabilities but were not taken seriously. The leak contains 122 records with hashed passwords.	SQLi
Feb 13		Trade.gov.cn	Inside what they call #OpChina, @RevolutionSec dumps 8000 accounts (usernames and hashed passwords) belonging to Chinese Government Trade website (trade.gov.cn)	SQLi
Feb 14		NORTEL NETWORKS	The Wall Street Journal reports that telecoms firm Nortel Networks was repeatedly breached by Chinese hackers for almost a decade. The newspaper cites Brian Shields, a former Nortel employee who led an internal investigation into the security breaches, and published claims that the hackers stole seven passwords from the company's top executives – including the CEO – which granted them widespread access to the entire Nortel network.	Unauthorised Access
Feb 15	L0NGwave99	NASDAQ	The L0NGwave99 Digital Group launches the "Operation Digital Tornado". In support of the "great and rooted 99% movement", the L0NGwave99 Group takes down the NASDAQ stock exchange besides a number of US stock markets. Taken down sites include: nasdaq.com, batstrading.com, cboe.com, ms4x.com, www.mynasdaqomx.com, www.esignal.com.	DDos

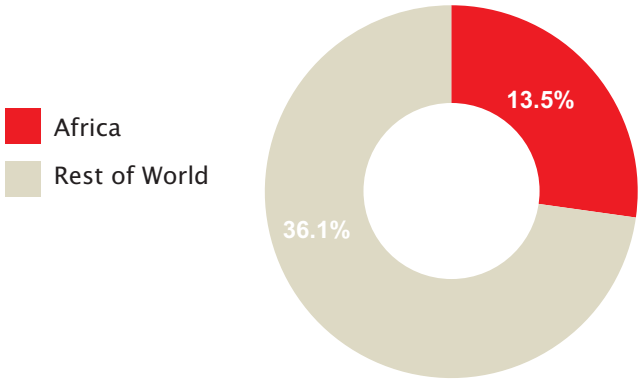
Date	Author	Target	Description	Attack
Mar 3	James Marks, James McCormick (suspected)	SONY	Sony confirms that Michael Jackson's entire back catalogue, including an unreleased collaboration with Will.I.AM, has been stolen by hackers after the breach in April 2011. Due to this breach the Sony Music archive was infiltrated by a couple of suspected persons, who illegally downloaded more than 50,000 digital files.	N/A
Mar 11			Senior British military officers, Defense Ministry officials, and other government officials were apparently tricked into becoming Facebook friends with someone masquerading as United States Navy admiral James Stavridis. By doing so, they exposed their own personal information (such as private e-mail addresses, phone numbers, pictures, the names of family members, and possibly even the details of their movements), to unknown spies.	Social Network Poisoning
Mar 30	Unknown	globalpayments™ MasterCard VISA	Global Payments Inc., which processes credit cards and debit cards for banks and merchants (among which Visa and Mastercard) is hit by a security breach putting 50,000 cardholders at risk (according to other evaluations, affected users could reach 10,000,000). According to rumors, the breached credit card processor was compromised between Jan. 21, 2012 and Feb. 25, 2012. The alerts also said that full Track 1 and Track 2 data was taken – meaning that the information could be used to counterfeit new cards.	Network Intrusion
Apr 1	Unknown	UTAH DEPARTMENT OF HEALTH	Unknown hackers break into the Utah Department of health and as a consequence anyone who visited the health care provider in the previous four months may be a potential victim of a security breach. The total amount of victims could hence reach 280,000 individuals with their social security numbers taken and 500,000 other individuals with less sensitive personal information like names, addresses and phone numbers stolen.	Unknown
Apr 5			Anonymous China keep on their devastating defacement campaign against hundreds of Chinese government and commercial websites. In a message left on one of the hacked Chinese sites – cdcbd.gov.cn, a home page for Chengdu's business district – the hackers expressed anger with the Chinese government for restrictions placed on the Internet.	Defacement
Apr 8	ANONYMOUS	TechAmerica	TechAmerica, a technology trade association announces to have been targeted by the Anonymous as it singles out supporters of Cyber Intelligence Sharing and Protection Act (CISPA), the proposed legislation to improve U.S. cybersecurity. Anonymous claimed credit for denial-of-service assault.	DDos
Apr 11			Members of the infamous hacktivist collective TeaMp0isoN target the UK's foreign intelligence organization, MI6, for accusing innocent people of terrorism, so they drop a 24 hour phone bomb on them. After the phone bombing stopped, TriCk, the leader of the group, calls the MI6 offices in London and starts making fun of them.	Phone Bombing

Date	Author	Target	Description	Attack
Apr 21		博讯新闻网	A massive attack takes down boxun.com, a website that has reported extensively on China's biggest political turmoil in years. The company is forced to move to a new web hosting service after its previous host said the attacks were threatening its entire business. He believes the attacks were ordered by China's security services, but it isn't clear where they were launched from.	DDos
Apr 26	Unknown	UK2.NET	UK2.NET, one of the most important hosting companies in the UK, is hit by a massive DDoS attack involving apparently a botnet composed by 10 million of unique IP Addresses.	DDos
May 2	Unknown	Ministry of Defence	Major General Jonathan Shaw tells the Guardian that Computer hackers have managed to breach some of the top secret systems within the U.K. Ministry of Defence (mod.uk)	APT
May 21	Unknown		One of the most well known billing and support systems for website control systems WHMCS (whmcs.com) is hacked by UGNAZI and as a result 1.7 Gb with data of 500,000 individuals are leaked.	Account Hacking
May 21	Kosova Hacker Security	IBM	IBM Research domain (researcher.ibm.com) is hacked and defaced by Hacker collective group dubbed Kosova Hacker Security.	SQLi
May 23	Alone Hacker	PMDB 15	The website of Brazilian Political Party PMDB do Maranhão (pmdbma.com.br) is hacked by an "Alone Hacker" who makes all the secondary pages of the web site inaccessible	N/A
May 24	Unknown	altrec.com	American Express notifies altrec.com that cards used on their e-commerce site had been compromised by unknown hackers on May 7, 2012	N/A

6 African Perspective

Whilst internet penetration in Africa still lags behind the rest of the world there is no doubt that it is seen as a priority to help improve the continent's competitiveness.

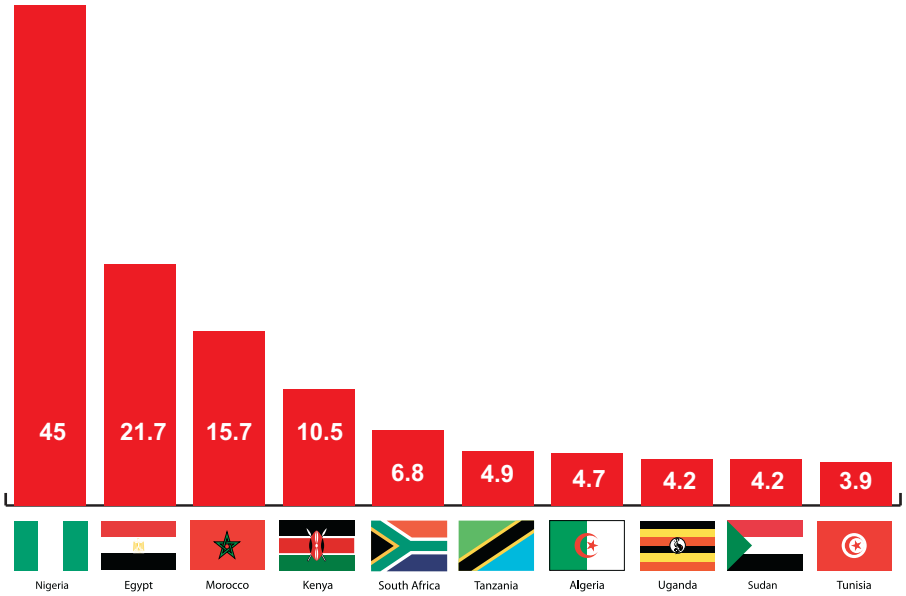
Internet Penetration in Africa December 31, 2011



Penetration Rate (% Population)

1 There are currently massive projects underway to connect Africa to the rest of the world. Whilst bridging the digital divide for economic and social reasons is an extremely essential step in the right direction it does come with risks.

Africa Top Internet Countries December 31, 2011



Millions of users

The African continent is particularly vulnerable to cyber security threats. With cheaper and faster Internet, more Africans will be "always-on" or continually connected increasing the number of "new" internet users that are not security-savvy. Cyber security is not a concept known to the vast majority, there is little understanding, knowledge and expertise and mostly a huge lack of awareness. Some of the reasons that have been cited for this lack of security awareness include shortage of local cyber security experts and the lack of funds.

Internet users, population and Facebook statistics for Africa

Africa	Population (2011 Est.)	Internet Users Dec/ 2000	Internet Users 31 Dec 2011	Penetration (% Population)	Users % Africa	Facebook 31 Mar 2012
Algeria	34,994,937	50,000	4,700,000	13.4 %	3.4 %	3,328,800
Angola	13,338,541	30,000	744,195	5.6 %	0.5 %	361,420
Botswana	2,065,398	15,000	167,180	8.1 %	0.1 %	199,180
Cameroon	19,711,291	20,000	783,956	4.0 %	0.6 %	481,280
Central African Rep.	4,950,027	1,500	123,800	2.5 %	0.1 %	105,580
Comoros	794,683	1,500	37,472	4.7 %	0.0 %	13,340
Congo	4,243,929	500	295,132	7.0 %	0.2 %	81,640
Congo, Dem. Rep.	71,712,867	500	915,400	1.3 %	0.7 %	643,220
Cote d'Ivoire	21,504,162	40,000	968,000	4.5 %	0.7 %	n/a
Egypt	82,079,636	450,000	21,691,776	26.4 %	15.5 %	10,475,940
Ethiopia	90,873,739	10,000	622,122	0.7 %	0.4 %	511,240
Ghana	24,791,073	30,000	2,085,501	8.4 %	1.5 %	1,205,420
Kenya	41,070,934	200,000	10,492,785	25.5 %	7.5 %	1,325,020
Lesotho	1,924,886	4,000	83,813	4.4 %	0.1 %	31,480
Libya	6,597,960	10,000	391,880	5.9 %	0.3 %	464,700
Madagascar	21,926,221	30,000	352,135	1.6 %	0.3 %	219,620
Malawi	15,879,252	15,000	716,400	4.5 %	0.5 %	127,780
Mauritius	1,303,717	87,000	323,494	24.8 %	0.2 %	312,640
Morocco	31,968,361	100,000	15,656,192	49.0 %	11.2 %	4,408,340
Mozambique	22,948,858	30,000	975,395	4.3 %	0.7 %	191,080
Namibia	2,147,585	30,000	148,414	6.9 %	0.1 %	148,420
Niger	16,468,886	5,000	128,749	0.8 %	0.1 %	43,880
Nigeria	155,215,573	200,000	45,039,711	29.0 %	32.2 %	4,312,060
Rwanda	11,370,425	5,000	818,048	7.2 %	0.6 %	127,680
Senegal	12,643,799	40,000	1,989,396	15.7 %	1.4 %	694,220
Seychelles	89,188	6,000	33,900	38.0 %	0.0 %	19,880
Somalia	9,925,640	200	106,000	1.1 %	0.1 %	75,500
South Africa	49,004,031	2,400,000	6,800,000	13.9 %	4.9 %	4,954,280
South Sudan	8,260,490	-	n/a	n/a	0.0 %	n/a
Sudan	45,047,502	30,000	4,200,000	9.3 %	3.0 %	n/a
Swaziland	1,370,424	10,000	95,122	6.9 %	0.1 %	62,540
Tanzania	42,746,620	115,000	4,932,535	11.5 %	3.5 %	437,040
Tunisia	10,629,186	100,000	3,856,984	36.3 %	2.8 %	2,955,260
Uganda	34,612,250	40,000	4,178,085	12.1 %	3.0 %	387,080
Zambia	13,881,336	20,000	882,170	6.4 %	0.6 %	206,700
Zimbabwe	12,084,304	50,000	1,445,717	12.0 %	1.0 %	n/a
TOTAL AFRICA	**1,037,524,058**	**4,514,400**	**139,875,242**	**13.5 %**	**100.0%**	**40,205,580**

(Source: http://www.internetworldstats.com)

Certain African countries have accepted this risk and started working on a national cyber security policy. Most however are lagging behind. African countries need to identify and mitigate their unique cyber security vulnerabilities and threats through joint initiatives and sharing of best practices. They also need to develop skilled resources through African Cyber Security Training Programs in collaboration with local and international role players and generate cyber security awareness at political, business, policing, education and society levels.

Cyber Security Role-Players on the African Continent

Economic Commission for Africa

The United Nations Economic Commission for Africa (UNECA) is addressing cyber security within the framework of the African Information Society Initiative (AISI). The establishment of the necessary cyber security organisational structures with national responsibility, including national CIRTs is still at construction level. According to UNECA, African governments are demonstrating increased awareness of cyber security issues, but existing capability to promote, monitor or pursue cyber security is relatively low.

Some African countries are now working with ITU, in collaboration with key partners, such as the International Multilateral Partnership Against Cyber Threats (IMPACT), to facilitate the development of cyber security capabilities, including the establishment of national CSIRTs.

Cyber Security Role-Players on the African Continent

African Network Information Centre (AfriNIC)	AfriNIC Government Working Group (AfGWG) is tasked to raise awareness among African governments and regulators on internet governance matters with a high emphasis on cyber security.
Global Cybersecurity Agenda (GCA)	A framework for international cooperation aimed at enhancing confidence and security in the information society launched by the ITU Secretary-General.
International Criminal Police Organization (Interpol)	World's largest international police organisation that facilitates cross-border police co-operation, further supports and assists all organisations, authorities and services whose mission is to prevent or combat international crime. INTERPOL created its Information Security Incident Response Team (ISIRT) in response to the increasing number of the targeted cyber attacks and information leakages. Part of the needs that are associated with cyber crime.
International Telecommunication Union (ITU)	Fundamental role to build confidence and security in the use of Information and Communication Technologies (ICTs) internationally.
IMPACT (International Multilateral Partnership Against Cyber Threats)	The world's largest United Nations - backed cybersecurity alliance. Functions as the cybersecurity executing arm of the United Nations' (UN) specialised agency for ICT - the International Telecommunication Union (ITU). Being the first comprehensive public-private partnership against cyber threats, IMPACT is the international platform which brings together governments of the world, industry and academia to enhance the global community's capabilities in dealing with cyber threats. IMPACT is the operational home of ITU's Global Cybersecurity Agenda (GCA). IMPACT with 144 partner countries is now formally part of the ITU-IMPACT coalition. IMPACT is a politically neutral platform, bringing together governments, academia, industry leaders, international organization, think tanks and cybersecurity experts to enhance the global community's capacity to prevent, defend against and respond to cyber threats.
Information Security Group of Africa (ISG Africa)	ISG Africa was created in response to the increase of information security threats facing companies in Africa. It consists of security professionals from corporate, government and IT or legal firms within Africa. ISG-Africa aims to provide a monthly forum for the exchange of Information Security related information and experience between members and further raise awareness of potential and identified vulnerabilities. ISG-Africa has active user groups in South Africa and Nigeria (www.isgafrica.org)

Southern African Development Community (SADC)	Mission is to promote sustainable and equitable economic growth and socio-economic development through efficient productive systems, deeper co-operation and integration, good governance, and durable peace and security. The proposed regional priorities for 2011-2012 includes, amongst others, the setting up of National and Regional Internet Exchange points and harmonisation of Cyber Security Regulatory Frameworks in SADC

The African Union Commission and UN Economic Commission for Africa collaborates with Regional Economic Communities such as SADC, COMESA, EAC and IGAD on Africa-wide harmonisation of cyber security Legislation, ICT policies and legal / regulatory frameworks.

A Draft African Convention on Cybersecurity seeks to harmonise African cyber legislations on electronic commerce organisation, personal information protection, cyber security promotion and cybercrime control.

In pursuance of the principles of the African Information Society Initiative (AISI) and the African Regional Action Plan for the Knowledge Economy (ARAPKE), the Draft Convention is intended to:-

1. Define the objectives and broad orientations for the information society in Africa.
2. Strengthen existing legislations in member states and the regional economic communities on Information and Communication Technologies.
3. Define the security rules essential to establishing a credible digital space in response to the major security related obstacles to the development of digital transactions in Africa.
4. Lay the foundation for cyber ethics and fundamental principles in the key areas of cyber security across Africa.
5. Define the basis for electronic commerce, puts in place a mechanism for combating intrusions into private life likely to be generated by the gathering, processing, transmission, storage and use of personal information and sets broad guidelines for incrimination and repression of cyber crime.

Its adoption would capitalise African and international experiences in cyber legislation and speed up relevant reforms in African States.

South Africa and International Co-operation

Bilateral Treaties	• Extradition Agreements exist with the following countries: Botswana; Lesotho, Malawi; Swaziland; Switzerland; United States of America; Canada; Australia; Israel; Egypt; Algeria; Nigeria; India; China; Namibia; Mozambique. • Mutual Legal Assistance Agreements exist with the following countries: Canada; United States of America; Lesotho; Egypt; Algeria; Nigeria; France; Chad;India; China; Iran; Namibia; Mozambique.
Regional Treaties	• SADC Protocol Against Corruption, 2002: signed and ratified; • SADC Protocol on Extradition and Mutual Legal Assistance in Criminal Matters, 2002: signed and ratified; • African Union Convention on Extradition: signed and ratified; • African Union Convention on Preventing and Combating Corruption, 2003: signed (16 March 2004) and ratified (11 November 2005); and • African Union Convention on the Prevention and Combating of Terrorism, 1999: signed (14 July 1999) and ratified (7 November 2002).
International Treaties	• UN Convention Against Corruption (UNCAC): signed and ratified; • OECD Anti-Bribery Convention: neither signed nor ratified; • Scheme Relating to Mutual Assistance In Criminal Matters within the Commonwealth • The London Scheme for Extradition within the Commonwealth (incorporating the amendments agreed at Kingstown in November 2002).
Other Treaties	• UN Convention Against Transnational Organised Crime and three Supplementary Protocols: signed and ratified; and • Council of Europe Convention on Extradition: signed and ratified.

Cyber Security Models and Initiatives in selected African Countries

According to the African Union, when looking at the reviewed countries' policy information, the most advanced country on this issue is Mauritius. Beside Mauritius, South Africa, Tunisia and Kenya are also actively working on their laws while others are putting their cyber security policies together. It is by no doubt then that, there is still an overall lack of security awareness and understanding of cyber security in Africa. Some of the challenges that are faced include: the lack of awareness and the shortage of local experts in the cyber security field. Most countries are willing to cooperate globally on the security of cyber space, but it is necessary to also collaborate regionally and learn from each other as well. An approved African cyber security policy will be one valuable step forward in the right direction.

Country	National Cyber Security Policy	National Cyber Security Awareness Programme	Organisations / Cybercrime Unit	CERT / CIRT	Member of FIRST	Budapest Convention Signed	Budapest Convention Ratified
BOTSWANA	• Cybercrime and Computer Related Crimes Bill 2007 (deals with issues of computer misuse, child pornography, combat cybercrime and computer related crimes, to repress criminal activities perpetrated through computer systems as well as to collect electronic evidence) • Financial Intelligence 2008 (deal with issues of money laundering, sponsorship of terrorist activities and any other fraudulent practices that may be undertaken both through the electronic and traditional over-the-counter means) • e-Legislation Committee in 2010 was formed and mandated to fasttrack the implementation of e-Legislation programme with particular focus on the development of key Cybersecurity laws • Start drafting the Information Protection, Electronic Commerce and Electronic Signature bills • Chapter 08:06 cybercrime and computer related crimes (An Act to combat cybercrime and computer related crimes, to repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence.	None	• Botswana Police Service (BPS) • INTERPOL National Central Bureau (NCB) • CCIPS (Computer Crime and Intellectual Property Section) • Member of IMPACT (International Multilateral Partnership Against Cyber Threats)	INTERPOL Incident Response Team (IRT)	No	No	No

Country	National Cyber Security Policy	National Cyber Security Awareness Programme	Organisations / Cybercrime Unit	CERT / CIRT	Member of FIRST	Budapest Convention Signed	Budapest Convention Ratified
BOTSWANA	Unauthorised access to a computer or computer system o Unauthorised access to computer service o Access with intent to commit an offence Unauthorised interference with information o Unauthorised interference with a computer or computer system o Unlawful interception of information o Unlawful possession of devices or information o Unauthorised disclosure of password o Damage to a computer or computer system o Protected computers o Cyber extortion, Cyber fraud o Electronic traffic in pornographic or obscene material o Unlawful disclosure by service provider						
GHANA	• Electronic Transaction Act (ACT 2008) that mandates the security agencies to confiscate accesses of cyber fraudsters; • Criminal Code Act 29/60 Section 131 for Cybercrime Prosecution • Ministry of Communications is currently drafting a national Cyber Security Strategy	e-Crime Project (e-Crime Bureau)	• The Commercial Crime unit of the CID of the Ghana Police Service • Internet Society Ghana Chapter (ISOC-Ghana) • SAKAWA organisation • INTERPOL National Central Bureau (NCB) • UK's Serious Organised Crime Agency (Soca) began work with the Ghanaian government in February to help it take technical steps to prevent cybercrime, and ensure offenders are prosecuted. • Member of IMPACT (International Multilateral Partnership Against Cyber Threats)	GH-CERT (Ghana's Computer Emergency Response Team)	No	No	No
KENYA	• Kenya Information and Communications Act CAP411A. • Kenya Communications Regulations, 2001 • Kenya Communications (Broadcasting) Regulations, 2009 • No National Cyber Security policy as yet however proposal in place that will include: o Collaboration between	None	• EACO – East African Communications Organizations (Cybersecurity Task Force) • National Cybersecurity Steering Committee (NCSC) • Criminal Investigation	• Kenya Computer Security Incidence Response Team (KE-CSIRT) • Kenya Computer Incident		No	No

Country	National Cyber Security Policy	National Cyber Security Awareness Programme	Organisations / Cybercrime Unit	CERT / CIRT	Member of FIRST	Budapest Convention Signed	Budapest Convention Ratified
KENYA	stakeholders; o Develop relevant Policies, Legal and Regulatory frameworks; o Establish national CERT thus providing a Trusted Point of Contact (TPOC); o Build Capacity: technical, legal and policy; o Awareness creation is key; o Research and development; o Harmonization of Cybersecurity management frameworks at the regional level (at the very least).		department (CID) and • Communications Commission of Kenya (CCK) • Jointed venture between ITU and the Communications Commission of Kenya • Cybercrime Unit (of the Police Force) • INTERPOL National Central Bureau (NCB) • Member of IMPACT (International Multilateral Partnership Against Cyber Threats)	Response Team Coordination Centre (KE-CIRT/CC)			
MAURITIUS	• Cyber Security Strategy include: • National Awareness Programs and Tools • Good Governance of Cyber Security & Privacy • Harnessing the Future to Secure the Present (Premier centre for cyber security, dependability and privacy, unique comprehensive approach, CyLab initiatives) • Personal Cyber Security (Home PC Security, Password Security, Child Safety Online, Social Engineering, Identity Theft, Road Warriors, Email Security) • A holistic approach integrates many elements (both strategic and tactical, both technical and non-technical, both professional and public)	• MySecure-Cyberspace, The Portal • Privacy Bird and Privacy Finder • MySecure-Cyberspace, The Game • CyLab engages in numerous partnerships and educational initiatives throughout the world • CERT-MU organising training/workshops for CIOs and System administrators; security awareness campaign for home users	• National Cybercrime Prevention Committee (NCPC) • INTERPOL National Central Bureau (NCB) • Member of IMPACT (International Multilateral Partnership Against Cyber Threats)	• Computer Emergency Response Team (CERT-MU) • Computer Incident Response Team (CIRT)	Yes	No	No
MOROCCO	• Morocco Numeric 2013 o Act No. 07-03 (completing the penal code regarding crimes related to treatment systems Automated Information) o Law No. 53-05 (concerning the electronic exchange of legal information) o Law No. 09-08 (protection of individuals with regard to processing of personal information) o Morocco in 2010 Numeric (Protect individuals with regard to the processing of personal information, promote paperless electronic transactions and support the development of	• FOSI's Global Resource and Information Directory (GRID) is designed to create a single, factual and up-to-date source for governments, industry, lawyers, academics, educators and all those dedicated to making the Internet a safer and better place	• Information Systems Security Committee within the National Council of Information Technology and Digital Economy • Committee on Safety of Information Systems; • The National Commission for Protection of Personal • INTERPOL National Central Bureau (NCB)	• MA-CERT (Computer Emergency Response Team)	No	No	No

Country	National Cyber Security Policy	National Cyber Security Awareness Programme	Organisations / Cybercrime Unit	CERT / CIRT	Member of FIRST	Budapest Convention Signed	Budapest Convention Ratified
MOZAMBIQUE	electronic commerce o National Cybersecurity Management System (NCSecMS), currently in the process of being implemented which consists of four components: the National Cybersecurity Framework, Maturity Model, Roles & Responsibilities and the Implementation Guide • Electronic Transactions Act, which deals with e-business and cybercrime	No	• INTERPOL National Central Bureau (NCB) • Member of IMPACT (International Multilateral Partnership Against Cyber Threats)	No	No	No	No
NAMIBIA	• Computer Misuse and Cybercrime Act 2003 f3 o Unauthorised access to computer information o Access with intent to commit offences o Unauthorised access to and interception of computer service o Unauthorised modification of computer material o Damaging or denying access to computer system o Unauthorised disclosure of password o Unlawful possession of devices and information o Electronic fraud • Prevention of Organised Crime Act no 29 of 2004 the court may hear evidence which might otherwise be inadmissable as long as trial is fair (sec 2(8) document means any record of information (sec 87 (4) electronic information inadmissable" "document" "information" "information". • Electronic Transactions and Communications Bill (to provide for the regulation of electronic transactions, communications and information systems management.	No	• INTERPOL National Central Bureau (NCB) • Member of IMPACT (International Multilateral Partnership Against Cyber Threats)	No	No	No	No

Country	National Cyber Security Policy	National Cyber Security Awareness Programme	Organisations / Cybercrime Unit	CERT / CIRT	Member of FIRST	Budapest Convention Signed	Budapest Convention Ratified
NIGERIA	• Harmonized Cybersecurity Bill 2011, for transmission to the National Assembly for passage as an executive bill. Scope of this Act are to o Part I – provide an effective, unified and comprehensive legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; o Enhance cybersecurity and the protection of computer systems and o networks, electronic communications; information and computer programs, Intellectual property and privacy rights; o Part II – criminalizes specific computer and computer – related offences and penalities. o Part III – provides for the security and protection of critical information infrastructure. o Part IV – deals with issues such as jurisdiction, powers of search and arrest, obstruction of law enforcement officers, prosecution, forfeiture of assets, compounding of offences; payment of compensation; and the power to make regulations. o Part V – deals with International cooperation o The Advanced Fee Fraud and other Fraud related offences Act was passed in 2006 (prescribed ways to combat online scams and other related cybercrimes by stating harsher penalties of imprisonment of at least 5years and at most 15 years without the option of a fine	Nigerian Cyber-Crime Working Group (NCWG) Initiative	• Nigeria Cyber Crime Working Group (NCWG) • INTERPOL National Central Bureau (NCB) • Partnered with the Queensland Police Department • The Economic and Financial Crimes Commission (EFCC) • Nigerian Cyber-Crime Working Group (NCWG) Initiative • Member of IMPACT (International Multilateral Partnership Against Cyber Threats) • ISG Africa • Information Security Society of Africa – Nigeria	No	No	No	No
SUDAN	• Cyber Crime Law of 2007 • Electronic Transactions law – 2007 contains Electronic contracting, Transactions-decadal, Digital signature, Electronic instruments. • Informatics Crimes law 2007 contains crimes on money , information , communications and the threat or blackmail; access to sites and information systems owned by the non; crimes of public order and	CERT Sudan	• Partnership with Amanak, ITU, IMPACT, OIC-CERT • INTERPOL National Central Bureau (NCB) • Member of IMPACT (International Multilateral Partnership Against Cyber Threats)	CERT Sudan	No	No	No

Country	National Cyber Security Policy	National Cyber Security Awareness Programme	Organisations / Cybercrime Unit	CERT / CIRT	Member of FIRST	Budapest Convention Signed	Budapest Convention Ratified
TUNISIA	• National Plan and Strategy in IT Security (2003) • Law on protection of Privacy and Personal information (Law No 2004-63) • Law on Electronic Signature and e-commerce (Law No 2000-83) • Law Against Cyber-Crimes (Law No 99-89) • Laws on consumer protection and Intellectual property • Law related to IT Security (Law No 2004-5, Feb 2004) Other law Amendments, under study: • Special amendments for Fighting Spam • Amendment of the law concerning Cyber-Crimes (Responsibilities of actors (ISP, Web Editors, Web authors, Access Providers) & Lawful Interception considerations (Cyber-Terrorism)	• CERT/Tunisian Coordination Centre • Specialized Mailing-list rubrics • Permanent rubrics in Regional and National radio stations • Presentations in All Third-party Conferences & Workshops • Presentations for public controllers & auditors	• Corporate -ISAC (IDCs) • INTERPOL National Central Bureau (NCB) • Member of IMPACT (International Multilateral Partnership Against Cyber Threats)	• Tunisian Computer Emergency Response Team (tunCERT); • CERT-TCC (Computer Emergency Response Team - Tunisian Co-ordination Centre) and in-corporates a CSIRST	Yes	No	No
ZIMBABWE	No law on cyber crime	None	• Criminal Investigation Department (C.I.D) Serious Frauds • Computer society of Zimbabwe • Member of IMPACT (International Multilateral Partnership Against Cyber Threats)	No	No	No	No

7 South African Perspective

The intention of this section of the project was to collaborate with key local and international stakeholders to obtain a clearer understanding of the current threat landscape. We also wished to analyse the challenges facing our teams dealing with cybercrime as well as which initiatives and cyber threat countermeasures would be optimal for the South African environment.

As a follow on from this report we will facilitate the establishment of task teams to investigate these initiatives in greater detail and encourage the forging of relationships and better collaboration across all relevant sectors.

For this report we interviewed experienced individuals and teams across the government, banking and telecommunications sectors plus obtained input from other specialists in the field. Questions were structured across 4 sections, namely:

1. National Cyber Threat focus

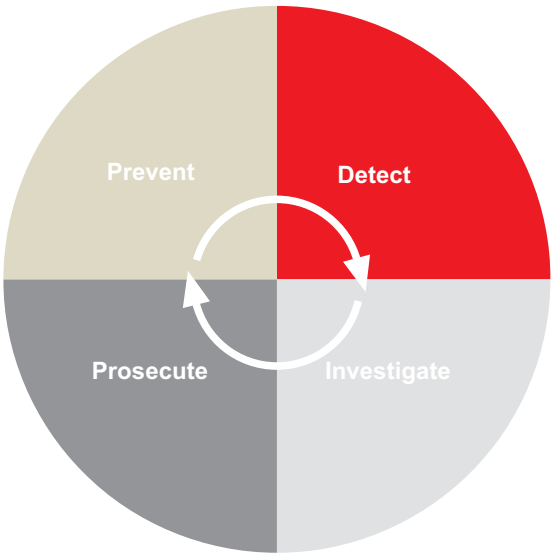
- Prevent
- Detect

2. Cybercrime focus

- Investigate
- Prosecute

"We used to look for a needle in the haystack... and now we are trying to find the most dangerous needle in a stack of needles", Donald Rumsfeld – Former US Secretary of Defence

- **Mitigation controls to prevent the attacks**
- **Collaboration of parties to assist with management of attacks**



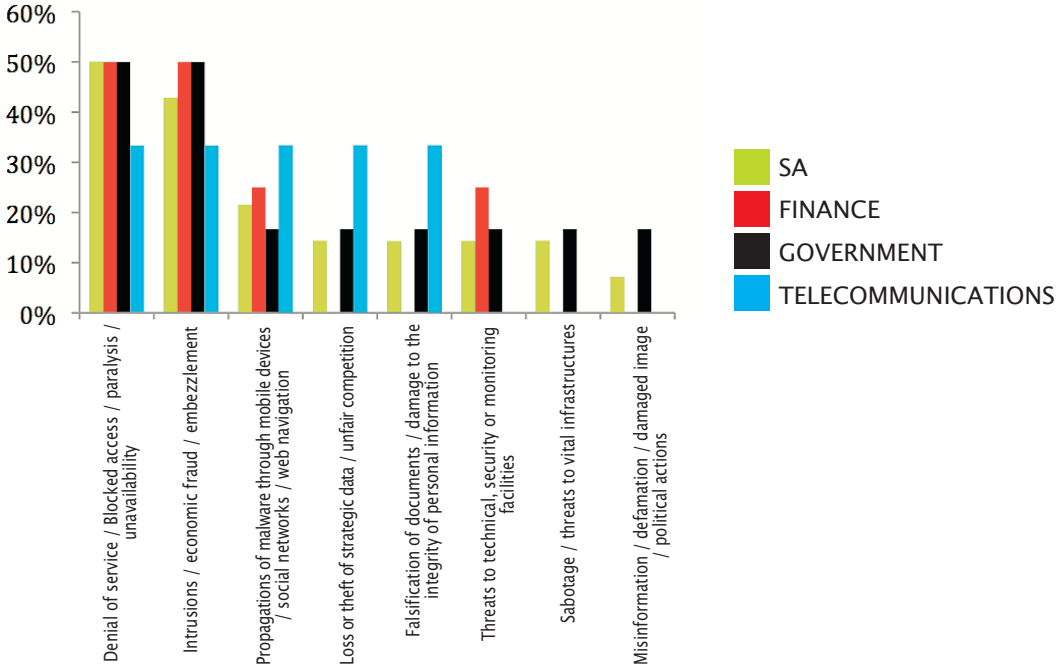
- **Identifyng attack methods and weaknesses exploited**
- **Investigating numerous cyber case studies**

- **Review of effectiveness of current legal system**

- **Perpetrator motives**
- **Law enforcement's ability to respond and investigate**

We furthermore extended a draft report of our findings to a larger pool of specialists for debate and ultimately validation of our analysis. We are therefore confident that the report accurately reflects the general sentiment of the South African cyber security and cybercrime stakeholder communities.

1. Which do you believe are the top 3 potential cyber threats to
1) SA and to
2) your industry?



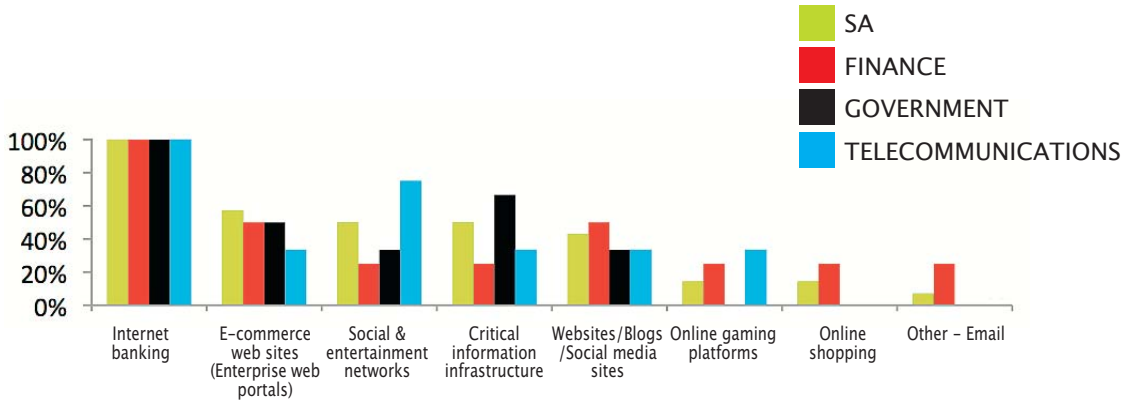
Commentary

The threat of denial of service (DOS) attacks and the unavailability of ICT were cited as the highest potential cyber threats affecting the Finance and Government sectors and ranked highly for the Telecommunications sector as well. Given the increased capacity of the various undersea cables linking South Africa to the world and the rapid increase in mobile communications, a large-scale DOS could result in severe degradation of services in South Africa should the country be targeted.

Intrusions and economic fraud were ranked as the second highest potential cyber threat to SA. System penetrations, privilege escalations to conduct fraud, fraud through SIM swaps and social engineering are seen more often as ways to steal money.

Finance Sector	Government Sector	Telecommunications Sector
Stealing of confidential information and the leakage of sensitive documents is a real concern for SA. Although financial gain is the prime motivator for today's fraudsters, personal data that can be used to facilitate other crimes is also being targeted to a greater degree than in past years South Africa organisations, particularly SME's are behind on implementing the protection of systems and the information that reside on them. It is apparent that modern technologies have changed the threat and vulnerability landscape and organisations have not fully come to terms with these changes Humans are the weakest link – Social engineering is the problem	It was noted that senior management must take responsibility for the information stored or used by the organisation. The information needs to be classified by the data owner and they are responsible for the classification so that the relevant security measures can be put in place to protect it The IT departments do have responsibility in that they need to ensure that the technological security measures are performing correctly Risk cannot be outsourced and service providers should be explicitly bound by contract to provide security services. It was suggested that providers, for example cloud computing service providers, should be responsible for the integrity of their infrastructure This is cause for concern due to the lack of security awareness and with the influx of new broadband subscribers may result in a rise in cybercrime and attacks	Loss and theft of strategic data and the falsification of documents resulting in the damage to the integrity of personal information is particularly a concern for the telecommunications sector The propagation of malware through mobile devices, social networks and web navigation (due to the increased use of mobile phones in South Africa) provides previously unconnected individuals internet access, contributing to the 25% increase in internet usage year over year SIM cloning has been raised as an increased concern in cybercrime incidents in South Africa to intercept communications between the online bank and the target

2. Which do you think are the top 3 targeted cyber services in SA?



Commentary

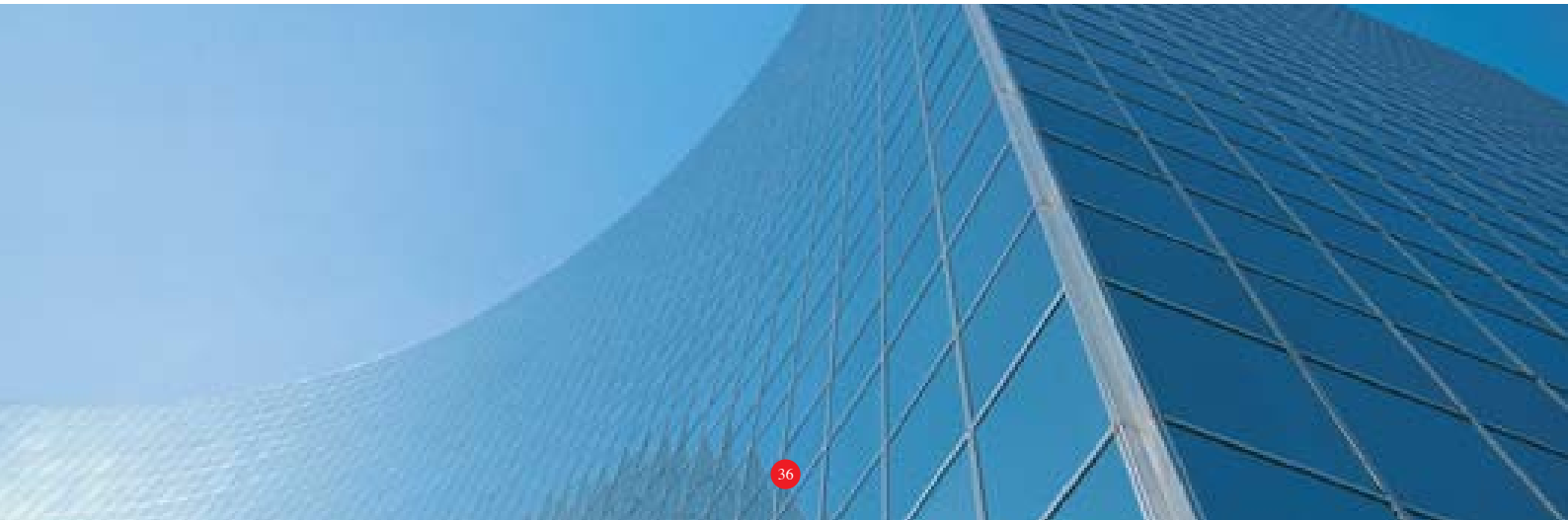
The weaknesses of digital identity management and the ability to use false identities to tap into global credit card and financial networks will continue to make this form of fraud attractive to cybercriminals. Although improvements in software and security technology have reduced some areas of risk, social engineering will continue to provide opportunity for crime and new technological vulnerabilities. (McAfee Virtual Criminology Report)

At number 2 on the list of most targeted services, ecommerce web sites including enterprise web portals (Internet facing corporate websites) are being targeted as more organisations and systems are dependent on the Internet and the need for protection has been cited as crucial.

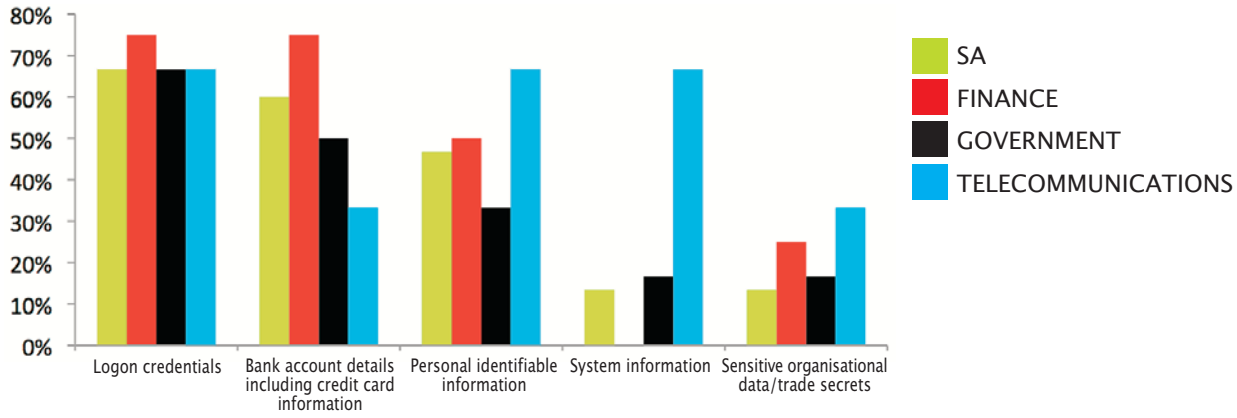
Social and entertainment networks such as Facebook hit the top 3 list. As mentioned previously the combination of social networks and mobile devices plays a significant role in aiding internet related fraud. Threats to vital infrastructures of this country made it to the top 4 list of potential cyber threats.

At number 5 was websites, blogs and social media such as Twitter for example has also shown to be a vector for attacks and malware infection.

Finance Sector	Government Sector	Telecommunications Sector
Internet banking still remains the number 1 targeted cyber service in all sectors in SA Social engineering is a niche target method and still a concern as well as an increase in spear phishing	Damage to critical infrastructure may result in severe degradation or cessation of operational capabilities, service delivery, the national economy, public health or national safety or any combination of this Critical infrastructures are critical to the well-being and functioning of a nation, society, or an organisation	The expected availability of social media by employees and breaches of confidentiality through this medium are of particular concern in the Telecommunications sector Defacements of websites in still a concern



3. Which information assets are most often targeted or compromised during a cyber attack against a SA organisation?



Commentary

The weaknesses of digital identity management and the ability to use false identities to tap into global credit card and financial networks will continue to make this form of fraud attractive to cybercriminals. Although software and security technology has improved, logon credentials are the main information asset targeted or compromised during a cyber attack.

Following this are bank account details including PINs, one time passwords, client profiles such as beneficiaries and credit card details continues to be a target in SA, despite the advancement and innovation in authentication technology.

Personally identifiable information is the 3rd most sought after information asset and highlights privacy concerns are becoming a high priority in SA. We believe this will further increase in importance once the Protection of Personal Information (PoPI) bill is enacted.

Finance Sector	Government Sector	Telecommunications Sector
The primary focus of malware is seen to be one of harvesting of account login details for criminal intent Fraud (and theft) is not only committed for financial gain but also to obtain sensitive organisational and trade secret information	System information was also raised as a means to obtain inside information about systems in order to target specific systems for destruction or obtain specific information	While identity is the foundation for most modern business processes, the abuse of identity is the basis for most occupational fraud and cyber-crime occurrences

National Cyber Security Framework

Securing a country against cyber-attacks has today become one of government's highest priorities. To achieve this objective, networks and systems, as well as the operations teams that support them, must vigorously defend against a variety of **internal and external threats**.

To respond to those attacks that are successful, defences must be prepared to detect and thwart follow-on attacks on internal enterprise networks as attackers spread inside a compromised network. A critical component of such a defence system is the establishment of a **National Cyber Security Framework** and to utilise continuous monitoring—that is, the ability to automatically test and validate whether current security measures are working and proactively remediate vulnerabilities in a timely manner.

A central tenet of cyber defence is that "offense must inform defence!"

In other words, knowledge of actual attacks that have compromised systems provide the essential foundation upon which to build effective defences.

Because government departments and companies have limited resources, current and past government chief information officers (CIOs) and chief information security officers (CISOs) across the USA and Europe have concluded that the only rational way to meet these requirements is to jointly establish a prioritised baseline of information security measures and controls that can be continuously monitored using automated mechanisms.

Guiding principles for control areas

- Defences should focus on addressing the most **common** and **damaging** attack activities occurring today, and on those anticipated in the near future.
- Enterprise environments must ensure that **consistent controls** are in place across the organisation to effectively negate attacks.
- Defences should be **automated where possible** and periodically or continuously measured using automated measurement techniques.
- **Root cause problems** must be fixed in order to ensure the prevention or timely detection of attacks.
- **Metrics** should be established that facilitate common ground for measuring the effectiveness of security measures, providing a common language for **executives, IT specialists, auditors,** and security teams to communicate about risk within the organisation.

The two tried and tested models we highly recommend for consideration by African stakeholders are:

Cyber security framework	Author / Endorser
1. Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines http://www.sans.org/critical-security-controls/	SANS Institute Centre for Protection of National Infrastructure (CPNI UK) Homeland Security (USA)
2. 35 Strategies to Mitigate Targeted Cyber Intrusions http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm Australian Government Department of Defence Intelligence and Security	Defence Signals Directorate (DSD) – an intelligence agency in the Australian Government Department of Defence

1. Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines

This consensus document of 20 Critical Controls begins the process of establishing a prioritised baseline of information security measures and controls that can be applied across government and commercial environments. The consensual effort identifies 20 specific technical security controls effective in blocking currently known high-priority attacks as well as those attack types expected in the near future.
The automation of these Top 20 Controls will radically lower the cost of security while improving its effectiveness. The US State Department has already demonstrated more than 94% reduction in "measured" security risk through the rigorous automation and measurement of the Top 20 Controls.

Critical Control	Effect on Attack Mitigation
Critical Control 1: Inventory of Authorized and Unauthorized Devices	Very High
Critical Control 2: Inventory of Authorized and Unauthorized Software	Very High
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
Critical Control 4: Continuous Vulnerability Assessment and Remediation	Very High
Critical Control 5: Malware Defences	High
Critical Control 6: Application Software Security	High
Critical Control 7: Wireless Device Control	High
Critical Control 8: Data Recovery Capability	Moderately High to High
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately to Moderatel High
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	Moderate
Critical Control 12: Controlled Use of Administrative Privileges	Moderate
Critical Control 13: Boundary Defence	Moderate
Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
Critical Control 15: Controlled Access Based on the Need to Know	Moderately Low to Moderate
Critical Control 16: Account Monitoring and Control	Moderately Low to Moderate
Critical Control 17: Data Loss Prevention	Low
Critical Control 18: Incident Response Capability	Low

These controls address operational conditions that are actively targeted and exploited by all threats

These controls address known initial entry points for targeted attacks

These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact

These controls are about optimizing, validating and/or effectively managing controls.

2. 35 Strategies to Mitigate Targeted Cyber Intrusions

The Defence Signals Directorate (DSD) has developed a list of strategies to mitigate targeted cyber intrusions. The list is informed by DSD's experience in operational cyber security, including responding to serious cyber incidents and performing vulnerability assessments and penetration testing for Australian government agencies.

Below are the top 4 (out of 35) mitigation strategies to focus firstly on computers used by employees most likely to be targeted by intrusions and then for all users. Additional mitigation strategies can then be selected to address system security gaps to reach an acceptable level of residual risk.

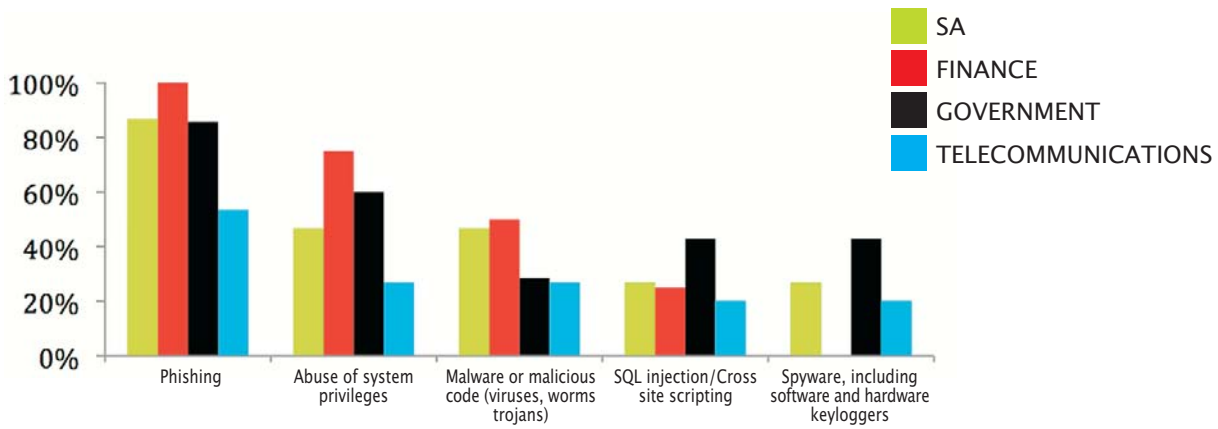
	Mitigation Strategy
1	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications.
2	Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version.
3	Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing.
4	Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker.

Action Plan

Given that these critical controls so closely track current threats and attacks, we recommend that CIOs and CISOs consider several immediate actions to ensure the effectiveness of their security programs:

1) Conduct a gap assessment to compare the organisation's current security stance to the detailed recommendations of the critical control
2) Implement the "quick win" critical controls to address the gaps identified by the assessment over the next one or two quarters
3) Assign security personnel to analyse and understand how critical controls beyond the quick wins can be deployed in the organisation's environment
4) Devise detailed plans to implement the more advanced controls over the next year

4. Based on your knowledge what are the top 3 common attack methods used against organisations in SA?



Commentary

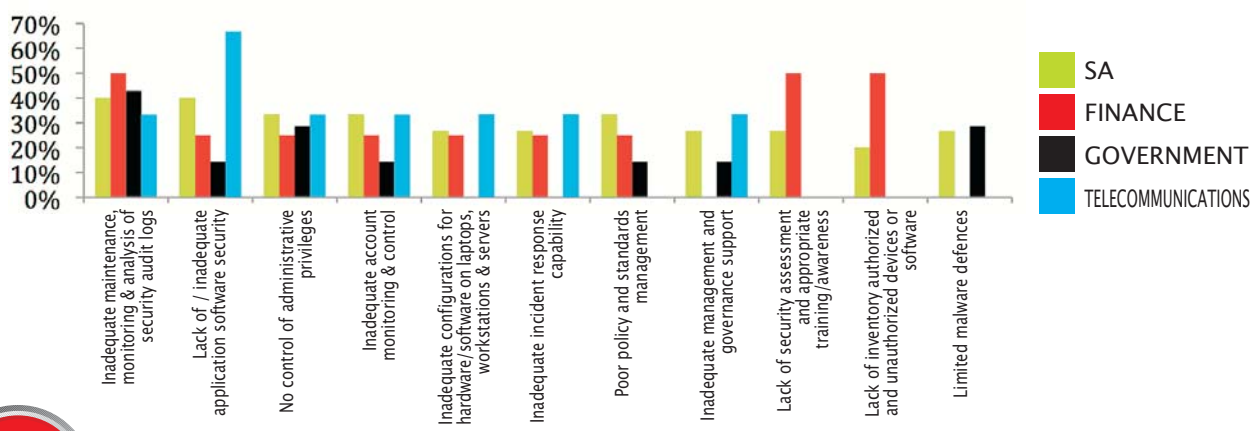
Despite increased sophistication in other types of cybercrime methods phishing still remains the most common attack method targeting most sectors in SA. Phishing attacks utilise spam emails to coerce or trick users to go to fake sites and enter their online credentials. A modification on this is the chat-in-the-middle attack, where a fake technical support instant messaging chat window is used to trick the user into providing account information. These attacks primarily target online banking to gain access to the victimí s finances.

Inadequate control and abuse of system privileges was the 2nd most common method of attack in SA and more popular in the Finance and Government sectors. The abuse of privileged access by external service providers, third parties and contractors was seen as a factor in these types of attacks.

Malicious software (malware), 3rd on the list, is prevalent in South Africa and can be rated as having a very high likelihood of being used in an attack as it has been leveraged for both espionage and infrastructure attacks.

Finance Sector	Government Sector	Telecommunications Sector
SQL injection and cross site scripting are still the most common methods Malware used to create botnets, support cybercrime and have been used to conduct Denial of Service attacks Malware distributed by social media has also becoming a popular means of attack	Government departments (and in particularly procurement systems) are hot targets for business information theft by contractors and third parties who often are contracted privately. Inefficient Government internal processes without proper separation of duties are exploited to compromise controls Despite advances in security technology to block these, the use of spyware is still very prevalent in SA. This includes mostly software based but also still includes hardware keyloggers Remote management software is also increasingly being targeted	The concern was raised that the increase in broadband availability without an increase in security awareness will probably result in a spike in the prevalence of malware infections and successful scams The difficulty in verifying the validity of communications over mobile networks raises concerns of information integrity, particularly with regards to phishing attacks Mobile malware is growing in prevalence and examples have been detected where information theft or espionage is taking place

5. What do you think are the common top 5 cyber vulnerabilities in SA?



Commentary

Inadequate maintenance, monitoring & analysis of security audit logs has been cited as the most common vulnerability in most sectors in SA. User awareness was also raised as a serious issue. It was pointed out that some organisations are apathetic and only do the minimum to ensure compliance, whilst smaller businesses may have the perception that information security only applies to the larger organisations. These attitudes indicate that the current processes and technical information security controls would be largely insufficient to protect against cybercrime.

Finance Sector	Government Sector	Telecommunications Sector
Although pockets of excellence exist in the finance sector, there is a huge shortage of risk mitigation skills and not enough to cover all the issues The inadequate protection and control of devices on the network infrastructure leads to an increase in malware attacks In the finance sector, other top common vulnerabilities included lack of security skills assessment, appropriate training /awareness and the lack of inventory of authorised and unauthorised devices or software	In the government sector, other top common vulnerabilities included poor policy and standards management and inadequate management and governance support Where they exist, well defined policies are most often only implemented in the finance sector in SA. The problem is not the lack of policies but rather whether these policies have been implemented and are being monitored There is also a lack of sound management decisions. There is a shortage of both technical and management skills in the law enforcement agencies in SA Critical security logs are either not enabled or in most cases logs are either overwritten or not monitored due to lack of skills Lack of fraud detection for business transactions (i.e. beyond the infrastructure layer) SA is strongly influenced by the political and social economic landscape – trends indicate cybercrimes are often closely linked to corruption	Inadequate application software security is the main vulnerability in the telecommunications sector. Other vulnerabilities include: – inadequate control of administrative privileges, account monitoring & control, configurations for hardware/software on laptops, workstations & servers, incident response capability and management and governance support Ineffective policies allow for accidental or intentional breaches from insiders – often as a result of poor corporate attitude, a lack of capability and understanding, or by accident There is a huge shortage of skilled resources for the development of secure applications. Most applications are written with security as an after– thought with security requirements not brought in at the onset of projects

6. Malware Analysis

The term malware, short for malicious software, covers a vast array of cyber threats such as computer viruses, worms, trojans, rootkits, botnets, spyware and keyloggers.

The global threat landscape is evolving. Malware and potentially unwanted software have become more regional, and different locations around the world exhibit different threat patterns.

International trends

The numbers of new **malware** samples are growing at an alarming pace. According to security firm **McAfee** over 1.5 million new pieces of **malware** were identified in the second quarter of 2012. The company said that the figure built on what was already record growth in malware and was the highest it has seen in the last four years.

Symantec's July 2012 Cloud Intelligence report has revealed the following statistics for email spam and other cyber security threats:

- 1 in every 436.6 emails was considered malicious and carried a virus.
- 1 in every 340.9 emails contained malware attacks, marking a 0.023% decrease from June to July 2012.
- 2,189 malicious websites were blocked per day, an increase of 4.0% since June.

The RSA 2012 Cybercrime Trends Report claims their Anti-Fraud Command Center achieved several milestones including the shutdown of over 700,000 phishing attacks and launching the first commercial anti-phishing and anti-Trojan services in the industry.

Since the beginning of 2011 phishing attacks identified by RSA's Anti-Phishing service alone have caused businesses approximately $52.3 million in potential losses. In fact, globally RSA claims to have prevented over $7.5B in fraud.

In 2011 Microsoft added more than 22,000 signatures to detect key threat families. The Microsoft Security Intelligence Report (SIRv11) stated that less than 1% of all vulnerability attacks were against zero-day vulnerabilities; 99% of attempted attacks impacted vulnerabilities for which an update was available.

The following statistics were compiled for April 2012 alone using data collected from computers running Kaspersky Lab products:

- 280 million malicious programs were detected and neutralized;
- 134 million (48% of all threats) web-borne infections were prevented;
- More than 24 million malicious URLs were detected.

When malware was used to infiltrate data, 98% of the time it was paired with keylogging functionality (Verizon Data 2012 Data Breach Investigations Report). According to the same report, incidents involving hacking and malware were both up considerably last year, with hacking linked to almost all compromised records.

According to Paladion Labs 2011 Phishing Intelligence Report, the average life of a phishing site was 5-19 hours with an average of 10 victims supplying their credentials per site.

South African trends

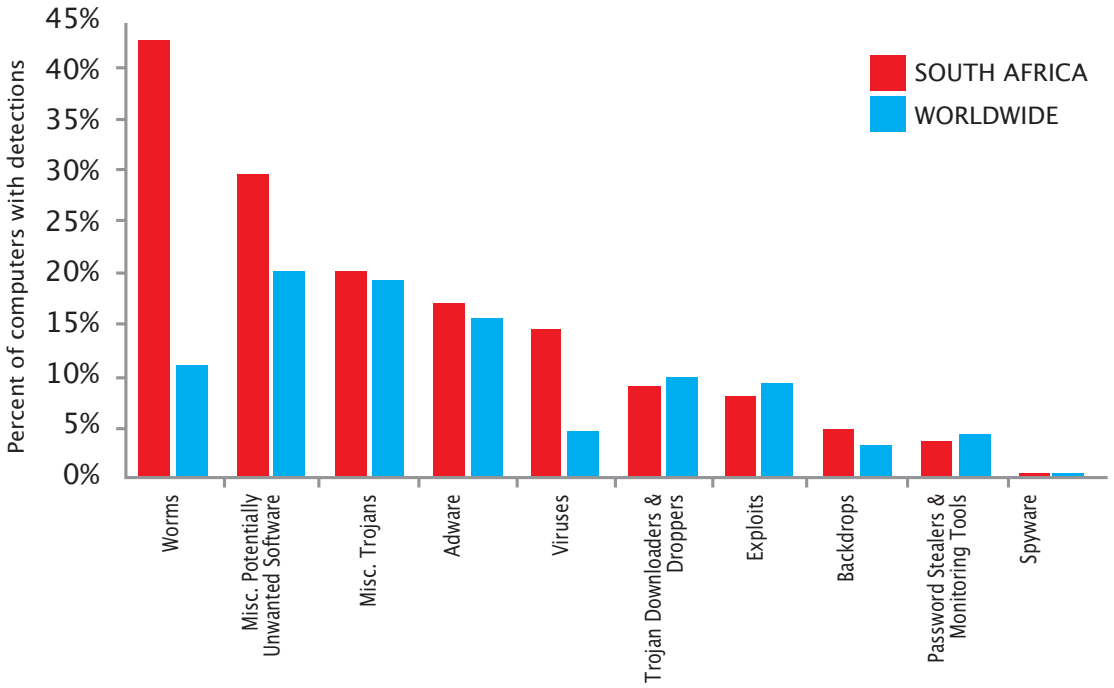
According to the Symantec Intelligence Report: June 2012:

- *South Africa was the second-most targeted country, with one in 170.9 emails identified as phishing attacks.*
- 1 in every 1.48 emails were considered spam, which made up 67.8% of all South African email traffic throughout July 2012.

RSA's Fraud Action service found that in June 2012 3% of all phishing attacks detected by RSA targeted South African brands.

In South Africa, the RSA Anti-Phishing service recorded a total of 1942 new phishing attacks with $6,828,072 in potential losses for the first half of 2012

The Microsoft Security Intelligence Report (SIRv11) shows the following malware and potentially unwanted software categories in South Africa in 4Q11, by percentage of cleaned computers affected:



Top 3 findings for South Africa:

- The most common category in South Africa in 4Q11 was Worms. It affected 42.8% of all computers cleaned there, down from 43.7% in 3Q11.
- The second most common category in South Africa in 4Q11 was Miscellaneous Potentially Unwanted Software. It affected 30.1% of all computers cleaned there.
- The third most common category in South Africa in 4Q11 was Miscellaneous Trojans, which affected 20.7% of all computers cleaned there.

7. What local initiatives are you aware of that involve collaboration to better deal with the growing cyber threat facing SA organisations?

Collaboration is an effective way to fight cybercrime – shared intelligence can prevent losses from occurring by enabling organisations to proactively combat known cybercriminals. An example is the RSA eFraudNetwork that allows South African organisations to collaborate on cyber threats such as identity theft or account takeover. It is a cross organisation repository of cybercrime data gleaned from RSA's extensive network of customers, ISPs, and third party contributors across the globe. When a suspicious pattern is identified, information such as the IP address and device fingerprints is moved to a shared data repository.

A number of collaboration initiatives should be considered for SA:-

- Cybercrime Legislation
- Computer Emergency Response Team (CERT/CSIRTs)
- Higher education programs
- End-user education
- Identity theft legislation
- National public key infrastructure
- System certification and accreditation
- Law enforcement / cybercrime partnerships across industries
- Standards and policies for system security

Finance Sector	Government Sector	Telecommunications Sector
Financial institutions are collaborating and sharing information through the SABRIC network of experts to combat organised crime. Part of the SABRIC mission is to build beneficial Private Public Partnerships (PPP) to optimise national economy of effort opportunities; and to enhance the critical mass of the PPP to the benefit of the banking industry through primary contracts, service level agreements and other partnerships An anti-phishing mailing group that pools and shares the latest information on phishing has been established. The mailing list also comprises ISP's, telecoms, universities and some private organisations. Through SABRIC an SA inter-banking CSIRT has also been established The Financial Services Board (FSB) convenes and facilitates meetings of the e-Commerce Advisory Committee (ECAC), an advisory committee to the Minister of Finance on matters to advance e-commerce in the financial services sector in South Africa. The ECAC comprises representatives from the National Treasury, Reserve Bank,	We need more local initiatives to share, work together and to partner in coming up with solutions We need a stronger body leading this and must not only be driven by government Implementation of cybercrime initiatives are very slow and not gaining ground There is minimal collaboration of law enforcement within government Government should be communicating basic standards and approaches There are pockets of collaboration between different groups/sectors but no central body Collaboration of efforts between CSIR, COMSEC, SAPS, Universities, SSA etc to bring together expertise, share experiences (good & bad) and assist in implementation of what works The SIU is trying to work on an initiative to get key stakeholders together to share/pool information The SA Cyber Security Academic Alliance	There is no formal collaboration within the Telecoms industry and between the banks The government's cyber policy is not seen as a collaborated effort for SA companies and only as a government initiative We are only aware of vendor projects and the ISG Africa initiatives to research collaboration possibilities in South Africa There is a lot of collaboration between key players such as ISG Africa, ISF and ISACA – to share experience and provide support. However we need more local efforts amongst our public and private sectors Recommendation of a national register where cyber threats are listed (prioritised and sanitised) is needed to assist the SA community as awareness is long overdue The Southern African Fraud Prevention Service (SAFPS) is a non-profit organisation established in 2000 and is principally engaged in the provision of an information exchange between subscribing Members, in order to detect,

Finance Sector	Government Sector	Telecommunications Sector
FSB, Department of Communications; Department of Trade and Industry, SA Police Service (SAPS); Financial Intelligence Centre; SABRIC, as well as two private sector representatives. The ECAC has accordingly identified cybercrime as the single biggest threat to e-financial services currently in South Africa	(www.sacsaa.org.za) is one initiative. SACSAA is an initiative between UJ, UNISA and NMMU The Centre for Cyber Security at the University of Johannesburg is another initiative. The main aim of this Centre is to establish a dedicated cyber security research/evaluation/teaching & training facility in SA and eventually further in Africa. The main offerings in the Centre at present in development are the Certificate in Cyber Security, the Cyber Crime Reporting Website and an advanced course in CIIP We need a Parliamentary Standing Committee for Cyber Security Oversight	avoid and limit fraud, thereby assisting crime prevention in the public interest. The pooling of information by SAFPS members serves to protect member organisations from the actions of criminals. SAFPS has generated fraud savings for members in excess of R5 billion since inception and houses some 36000 confirmed fraud listings

8. What research do you believe needs to be conducted to better deal with the growing cyber threat? Who should fund this research (Government, Private institutions or a combination of the two)

Government and private institutions each have a role to play in conducting and funding research. Private sector organisations are typically focused on near-term projects that will result in revenue generating opportunities whereas governments may take a longer-term view and have the resources to fund extended term projects. Improved collaboration between the government and the private sector will result in the most effective approach to research and development projects.

Finance Sector	Government Sector	Telecommunications Sector
Research around cloud security and legal issues as most cloud providers are not hosted in SA. Issues include level of security to apply, vendor lock-in threats, redeployment to another cloud and business continuity if the cloud is breached Risks in investing in African countries, engaging with African providers, controls they have in place and the security issues they are facing Status of SA regarding our vulnerabilities and incident response strategies for SA Research on social engineering and its impact in SA – human and digital phishing Emerging threats to SA and drivers for cybercrime Sharing of information must be real-time and current. The research conducted must include compromises, lessons learnt and most importantly operational security issues. Collaboration and sharing of information will yield better results. Everybody needs to take responsibility in contributing to combating cybercrime Communities/Industries must work together, pool information and share data which will add value	SA needs to invest in research and the development of academics Our policy framework must take research into account Research required on how to utilise evidence or support from sites such as Facebook or Google as prosecutors lack knowledge and tools in this area More research based on surveys such as the SA Cyber Threat Barometer There needs to be more willing contribution from government sources and a collaborative approach to pool knowledge. Research needs to be part of a central body of control to share information Research must be based on best practices and global trends and analysis Research on topical issues – such as ID theft, mobile threats etc Both government and private sector must fund the research Government deals with lots of other issues – housing, poverty etc and doesn't have the time/resource/skill for cybercrime issues Research on determining our current national security skills level so that we know where to focus Research needs to be done on ISPs and their responsibilities in protecting the nation	Emerging threats in SA and cyber-attacks as they are being identified, including trend analysis and potential weaknesses that South Africa can protect against Local trends on phishing and spam Research must be a collaboration effort between government and private institutions. With maturity participation should be extended to international countries governments and businesses who share South Africa's economic and financial interest Government should initially fund the research and let private sector run and drive it forwards Research must be conducted on what the emerging/realistic threats are, how we report cybercrime (i.e. definition and categories of cybercrime) and the level of skills we currently have in SA and how to close the gap

9. Do you believe that a National Computer Security Incident Response Team (CSIRT) needs to be established? Where do you believe this should be run from and which stakeholders should be involved?

Commentary

The lack of a functional national CSIRT in South Africa was identified as a major problem, as there is no centralised source of information to provide a clear view of cybercrime and cyber incidents in South Africa. The introduction of new legislation and standards in South Africa is expected to improve security governance by forcing organisations into compliance and disclosing data breaches.

However, as was continuously raised in the interviews, the focus in most companies is on increasing revenues and decreasing costs and security is still seen as a side-issue.

A concern is that there are only currently a few African nations with operational computer security incident response teams (CSIRTs): Kenya, Tunisia, and Mauritius to name a few with reports of other countries investing in capability. The introduction of a CSIRT should be prioritised as such a facility would provide much needed support to organisations in the country and provide a central point to co-ordinate responses in the event of an attack. Such a facility is also crucial to continuing research in information security areas. Whilst many government CSIRTs keep their information confidential, the high infection rates and low awareness situation in Africa indicates that CSIRTs need to play a more public role.

The CSIRT could contribute valuable information to a number of initiatives:

- increasing security awareness
- building national expertise in information security
- incident management and computer forensics
- enhancing cyber security laws
- provide a central trusted point of contact for cyber security incident reporting
- establish a national centre to disseminate information about threats, vulnerabilities, and cyber security incidents
- foster the establishment of and provide assistance to industry CSIRTs
- coordinate with domestic and international CSIRTs and related organisations and
- become an active member of recognised security organisations and forums
- collaborated response where lessons learnt will grow security response

The CSIRT should aggregate relevant & timeous security information and ultimately provide a 24 x 7 x 365 real-time response capability.

Finance Sector	Government Sector	Telecommunications Sector
There are pockets on information everywhere but we need to pool information and experience together to benefit as a country The private IT community can even offer free services to government and law enforcement in times of need A National CSIRT is required but must be driven by government for sustainability. It must be institutionalised as a function of the government. DOC should be driving it, with the inclusion of all government departments and the private sector	We need a National CSIRT where the biggest stakeholder is the government We need to create a Cyber Hub as there is currently no central/nodal point for cyber security It is Important to have a top-down approach with one National CSIRT so that we have control from a single point The CSIRT must be an independent body and not run by government only, especially intelligence agencies that may not be trusted We need a national CSIRT but also need	A national CSIRT is necessary but sectors CSIRTs are more important, must not be duplicated and must be sustainable South Africa does not have an operational CSIRT. This is considered a problem since there is no central body to co-ordinate responses or provides a holistic view of incidents in the country. Yes – However, many organisations will be reluctant to divulge their incidents even where law requires such declaration. I believe that once the benefits are realised, then there will

Finance Sector	Government Sector	Telecommications Sector
A National CSIRT is necessary to pull things together, but SA needs sector CSIRTs as well	community oriented CSIRTs It is time that we (in particular governments) start collecting incidents and measuring the impact of this crime and report it regularly as part of the National Crime Report / Statistics We need to study other CSIRT models internationally to build our CSIRT	be more support towards a CSIRT. Should be run from a neutral trusted entity

10. Do we need to establish a National Cyber Security Training Academy to address the country's cyber security requirements?

Security professionals are in high demand globally at a time when cyber attacks are increasing in both number and sophistication. A national cyber security training academy would help address the growing need for information security professionals at a national level.

The formation of a regulatory body to oversee the industry was proposed as a method of ensuring quality and consistency in security qualifications and competencies of professionals working in this field. Further introduction of information security into tertiary computing-related curriculum is also needed. Security requirements should be integrated into various topics and as was stressed in this research it is vitally important to include security in the development lifecycle as an example.

Finance Sector	Government Sector	Telecommunications Sector
Cybercrime is a wide field with room for expertise and specialist skills in different areas. However there should be a minimum standard which must be adopted. There should be bodies in place that determine the minimum baseline for compliance and recruitment The training needs to be practical and sustainable In terms of training there is no "ONE SIZE FITS ALL" approach with more of a tailored offering especially for cybercrime skills Existing training courses could be facilitated by current training institutions e.g. SANS SA Universities should be doing this and should partner with other universities internationally. The SA universities qualification must attract other African countries to complete a degree or certificate in SA. University courses to be updated to include secure application development	Training must be part of a university qualification and must be formal and credible Training should include an Executive Security Programme Training is a huge problem in SA. There is a Justice Training College run by the DOJ offering courses on RICA, but not enough training is done regarding cyber crime The Academy should be a body that is seen to be neutral, endorsed by both government and industry and recognised as being world class Yes, this is very important. Should be easily accessible to government and private companies with minimal red tape and procurement hurdles	National training for the country is lacking. Basic security training in SA is generally low Training should be done in association with the universities and at NQF level Universities should offer a Cyber Protection qualification that includes cyber defences Important to have a standard baseline/curriculum which is accredited and can be used as a benchmark A nation-wide security-aware culture needs to be set so that children are trained from a school / university level. Awareness topics to include protection of personal details and how to avoid ID theft

SA Cyber Security Academy

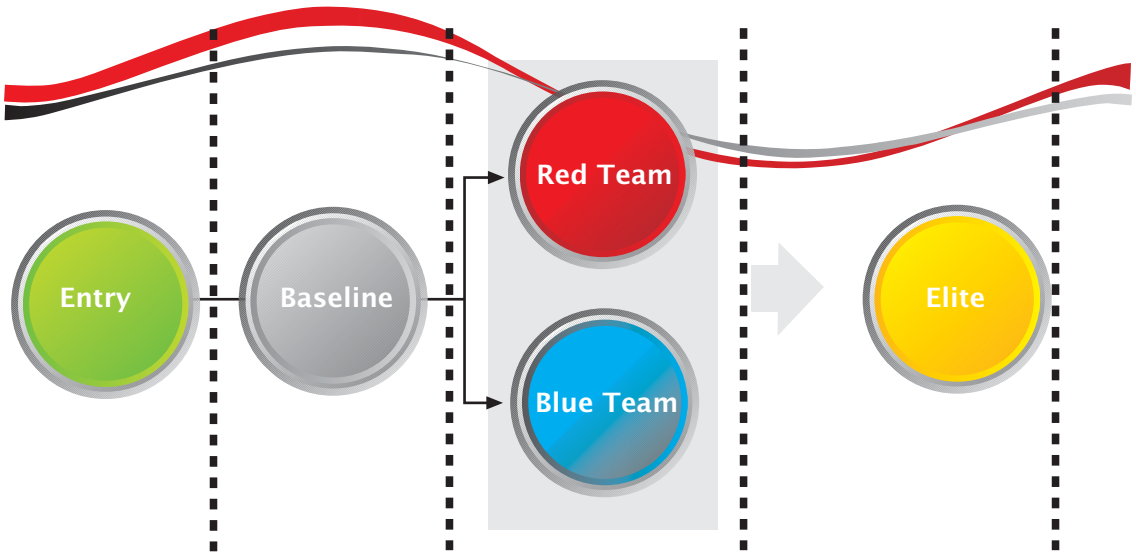
Cyber security professionals are involved in activities that include the security of operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities. This includes computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

A national cyber security training, awareness, and education programme must be based on a validated training strategy and include a formal curriculum in addition to other learning interventions.

We cannot dispute the fact that South Africa:

- needs greater cybersecurity awareness
- lacks sufficient cybersecurity experts
- has a number of training courses on offer but lack consistency and cohesion
- potential employees lack information about skills and abilities for cybersecurity jobs
- resources exist for teachers and students about cybersecurity but are difficult to localize
- cybersecurity career development and scholarships are limited
- there is a lack of communication between government, private industry, and academia

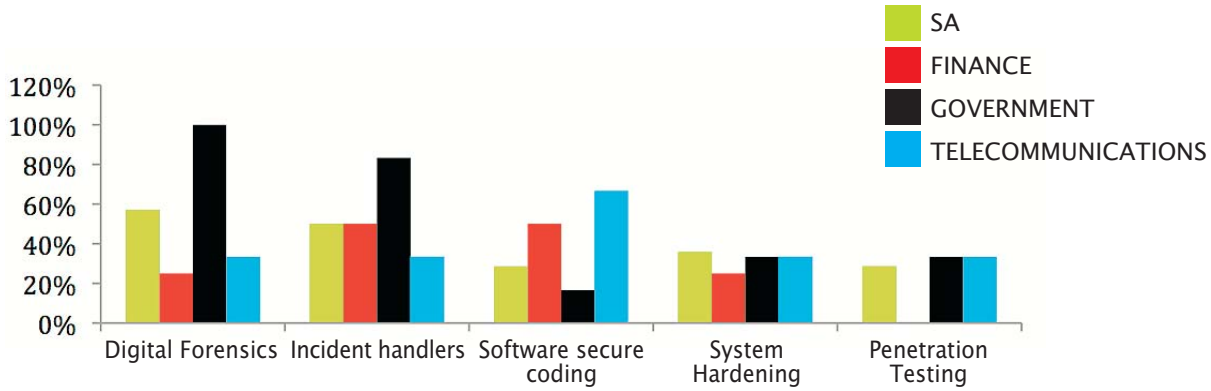
We propose the establishment of a National Cyber Security Academy to identify current skills and competency levels within the country (AS-IS), to determine the existing and future national requirements using a risk-based approach (TO-BE) and implement a continuous-improvement training programme to address the country's security obligation.



The programme needs to consider skills across the entire lifecycle.

Entry	A skills attraction & assessment programme to allow the easy introduction of school-leavers and graduates to enter the cyber security sector.
Baseline	Criteria to define the minimum required skills and competencies required for a junior cyber security professional. The proposed qualification would be endorsed by recognised industry professional bodies.
Blue team	The blue team's job of protecting information assets starts with designing, building, implementing and maintaining a robust cyber security programme within their organisation or industry.
Red team	The red team's job is straightforward: seek and penetrate. A red teamer will use every tool available to compromise a target network and gain entry to a blue team's defenses, with the ultimate goal of taking control of one or more critical systems in order to realistically test defenses in a simulated environment.
Elite	These elite teams of technical security professionals will be a small group of highly skilled cyber security special forces whose national responsibilities includes securing key-point systems, reconnaissance, counterterrorism and counter hacks where necessitated.

11. What cyber security skills do you believe are in short supply in your sector and SA?



Commentary

Cyber security skills in SA are definitely in short supply with digital forensic skills topping the list in all sectors in SA. These resources should be able to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions about the information related to cybercrime.

The second most scarce cyber security skill in SA were experienced incident handlers, who were able to respond to a variety of computer security incidents, such as unauthorised data access, inappropriate system usage, malicious code infections and denial of service attacks.

Finance Sector	Government Sector	Telecommunications Sector
Not only do we need more resources trained on how to analyse and retain digital data but also how to present electronic evidence so that it is permissible in a court of law There is also not enough secure software development skills There is lack of security practitioners who have a broad range of security skills from being able to perform system hardening to penetration testing The SANS TOP 20 controls course needs to be a mandatory baseline for all security practitioners	While the security of software can be attributed to the technologies chosen or processes followed, eventual accountability is ascribed to the people building it. Inherently secure technologies are limited and in cases when chosen, the likelihood that they are implemented securely is isolated. Many times, the processes that are implemented to aid in the security of software end up being circumvented, due to constraints in project scope, schedule and budget Many African countries understand security far better than SA As a result of the shortage of skills SA is more reactive as opposed to having a proactive, multi-layered intelligence driven approach to dealing with cybercrime issues	SA also has a skills shortage of deep technical skills in the security team, covering areas such as system hardening and malware analysiss. There is also a lack of crime combating, investigative and prosecutorial skills SA also lacks good cryptographers (cryptologists and analysts) skills to be able to hack and crack codes. SA universities do not offer technical crypto skills; they lack key technical computer security skills and only focus on soft skills such as information systems

12. Do you believe that a National Awareness programme needs to be conducted? Which stakeholders should be involved and which sectors should this first be communicated to?

Social engineering tactics (e.g. getting a prospective victim to click on a link or to divulge a password) often play a role in cybercrimes. A national awareness program could be highly beneficial in South Africa, where one survey found that 84% of adults in that country had experienced a cybercrime. (South Africa was second only to China, which experienced a 85% victimization rate.)

The 2011 Verizon Data Breach Report was cited as claiming that many breaches were avoidable and occurred due to incorrect implementation of security measures. This lack of awareness, combined with the apathy mentioned above, contributes to the significant financial losses incurred due to malicious cyber-activity. Awareness training and proper management of security controls would therefore reduce the financial impact firstly at a corporate level and ultimately then for the national economy.

Finance Sector	Government Sector	Telecommunications Sector
The weakest link in many instances is the consumer so awareness is a high priority. National awareness needs to be created but MUST be targeted to the relevant audience with the relevant messaging. A “one size fits all" or a single National Awareness Campaign approach doesn’t work. A National Awareness Program addressing phishing must be jointly funded by all the banks. The private financial industry needs to take responsibility for educating these banking clients The Finance industry thinks that mobile device companies need to do more to educate customer as more and more devices become internet enabled and are their primary internet device Similarly other industries must also take responsibility and have a role to play to raise awareness. Telecoms should deal with specific issues such as cyber bulling / sim swaps /etc.	As a nation we need to work holistically towards a common framework and the National Awareness Program must be a public-private partnership We need to plan carefully for the rollout of computers and cyber technology into non-IT literate society We need to include Basic, Intermediate and Advanced levels of awareness for business and home users , support staff, service providers and development staff as well as line, middle and executive level management "In the Online World, we should be trained to look right, left and right again before we cross the street". This type of general cyber awareness must be used across the company Stakeholders involved in the awareness strategy include SAPS , the SA Government and Private sector	Government has the overall responsibility for all SA citizens. The SA government must do the blanket approach for generic awareness similar to water conservation, saving electricity and preventing HIV Universities must also play a role in educating our children and parents The Department of Education must integrate cyber awareness into the curriculum A one week national awareness campaign is not enough and this must be a continuous all year round effort done by the relevant sectors SAPS might not have the resources but they carry authority and position in society. This can take a form of media sponsorship like the SABC for the awareness targeting vulnerable groups

8 Cybercrime Section

According to the 11th United Nations Congress of crime prevention and criminal justice the South African government acknowledged that 341 organised crime groups are known to be operating locally.

This organised crime is seen as a serious threat to the stability of the country and whilst there have been efforts to halt its progress; these have been compromised by the scale of corruption. A three year study by the Institute for Security Studies was damming in its conclusion: "This research has thus far found that corruption not only facilitates organised crime but is indeed an integral part of every type of criminal activity surveyed."

This does not imply that the country is in the grip of criminal networks, as some Latin American or West African states are, but the warning signs are there. Unless they are heeded the direction of travel is clear and the outcome would be disastrous for the country and the region.

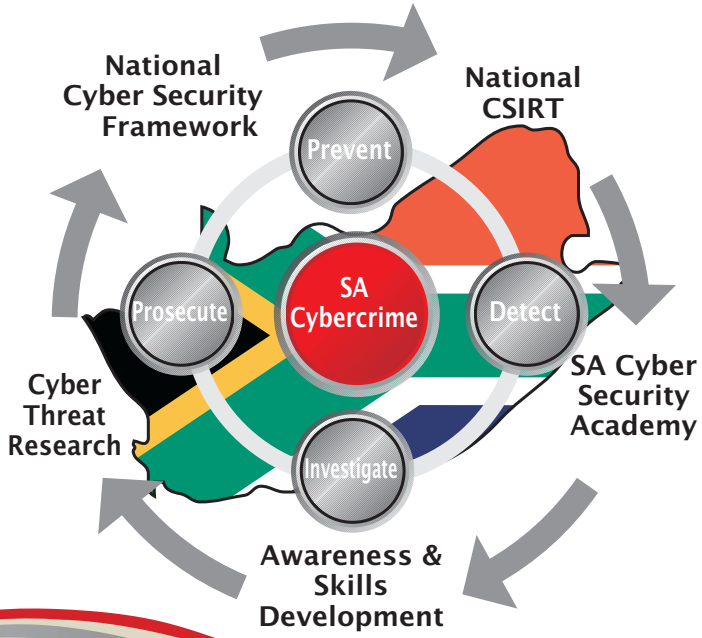
Definition of Cybercrime

Cybercrime refers to:-

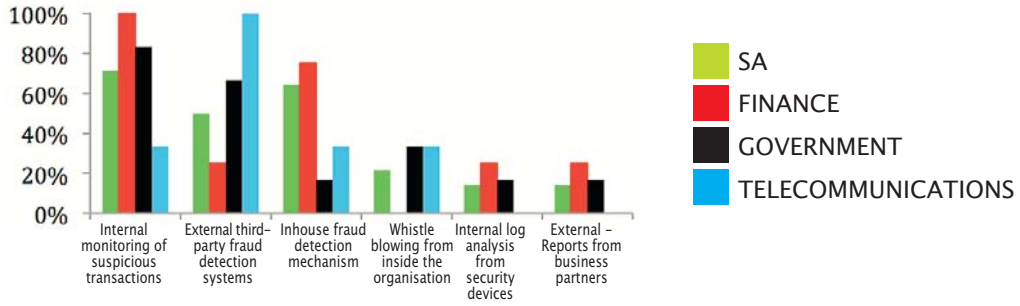
- *"illegal acts, the commission of which involves the use of information and communication technologies"* (National Cyber Security Policy for South Africa);
- *"access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data."* (Electronic Communications and Transactions Act of South Africa)

The criminalisation of illegal access, illegal interception, illegal data interference, illegal system interference, computer related fraud and forgery are the standard provisions in most cyber laws enacted in countries around the world.

Cybercrime is borderless by nature – this also makes criminal investigations more complicated for law enforcement authorities. To effectively tackle cybercrime, adequate crossñborder provisions are needed including international cooperation and mutual assistance.



13. From your experience what are the top 3 ways that cybercrime incidents are currently being detected? Where do we need to enhance this capability?



Commentary

For this question we provided a number of options to consider, namely:

Internal Corporate Policies / Controls

- Fraud detection mechanism
- Log analysis from security devices
- Rotation of personnel duties
- Monitoring of suspicious transactions
- Unusual system behaviour or performance

External Findings / Other

- Accidental/errors by end users
- Notified by law enforcement
- By media
- Contact from suppliers
- Customer notifications
- Reports from business partners
- Third-party fraud detection

Tip Offs

- Internal
- External
- Whistle Blowing

It was noted that organisations do not always have the capability to prevent or detect attacks. In many cases organisations only discover that their security has been breached when there was a noticeable irregularity, such as a large telephone bill that exceeds actual usage. It was also noted that many organisations were unable to implement basic information security controls effectively and were therefore unlikely to be able to implement more advanced security measures.

Even though organisations are aware of the importance of effective log management, many local companies do not have proper system logging processes in place, or do not monitor their logs consistently. This contributes dramatically to the majority of local companies not detecting security breaches in SA. An exception to the rule however is the finance sector which seems to be much better at monitoring and analysing logs for suspicious business transactions using a number of in-house fraud detection mechanisms.

External third-party fraud detection systems are starting to gain popularity in almost all sectors in SA, with popular products being the RSA eFraudNetwork, Symantec Security Operations Centre, Mcafee Strategic Security Services, Trusteer and Microsoft Malware Protection Centre to name a few.

Finance Sector	Government Sector	Telecommunications Sector
Sectors such as government and telecommunications largely depend on the mature fraud detection mechanisms within their financial institutions to help them detect fraudulent activity in their environments. Financial institutions have mature fraud detection and monitoring solutions, so often these are the last lines of defence to identify fraudulent activity The rise in targeted attacks appears related to cybercrime syndicates and the criminals themselves do not necessarily have the technical skills, but target one or more individuals who do have the necessary access or skills. These individuals may then be bribed or threatened to help target victims	The main threats discussed were insider threats from current and ex-employees, crime-syndicates and targeted attacks. It was indicated in cases that disgruntled employees who left an organisation, may intentionally copy or release sensitive information to damage the organisation concerned It was raised that in most instances of fraud the perpetrator was found to be an associate of an employee in the victim organisation	The telecommunications sector also highlighted the lack of fraud detection for business transactions beyond the infrastructure layer Internal whistle blowing in the government and telecommunications sectors were also noted as important tools to exposes fraud and corruption

14. Are cybercrime occurrences increasing in South Africa?

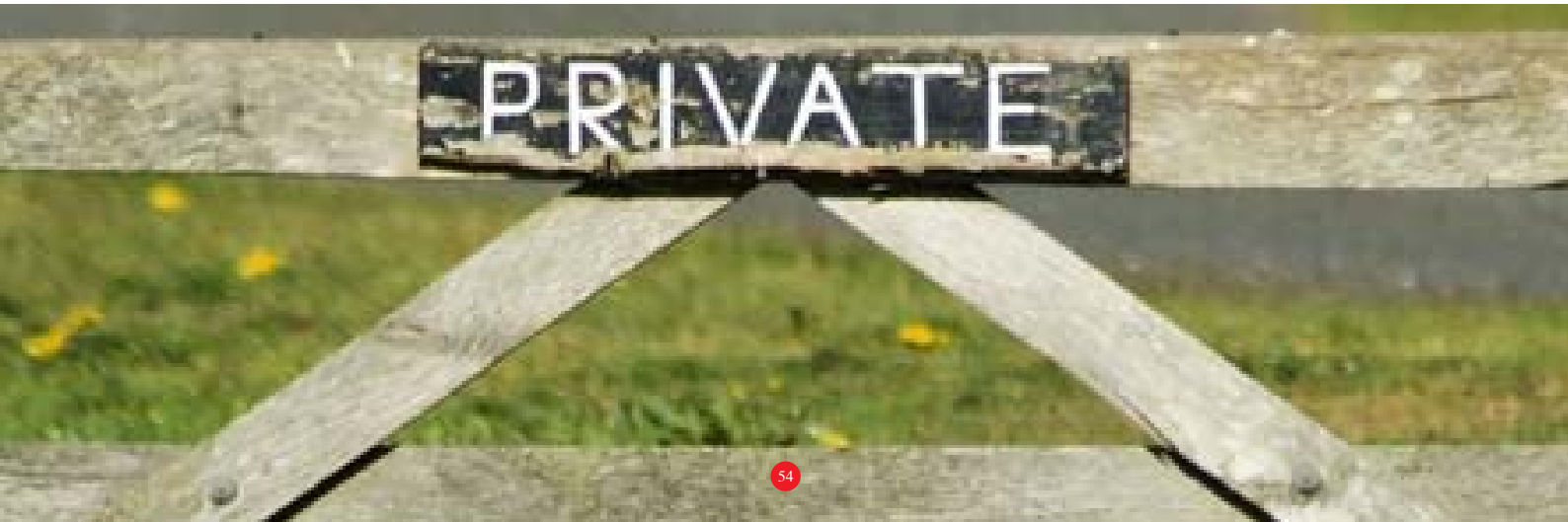
Commentary

In their latest 2012 Norton Cybercrime Report, Symantec claimed that cybercrime is enjoying exponential growth at rates never seen before:

- 556 million victims per year = 1.5+ million victims per day = 18 victims per second
- The global price tag of consumer cybercrime is $110 Billion (The cost Americans spend annually on fast food)

Whilst we cannot provide an accurate figure to the cost of cybercrime in South Africa we can state that based on input from the stakeholders we interviewed there is no doubt that activity in all sectors has definitely increased from 2010 onwards.

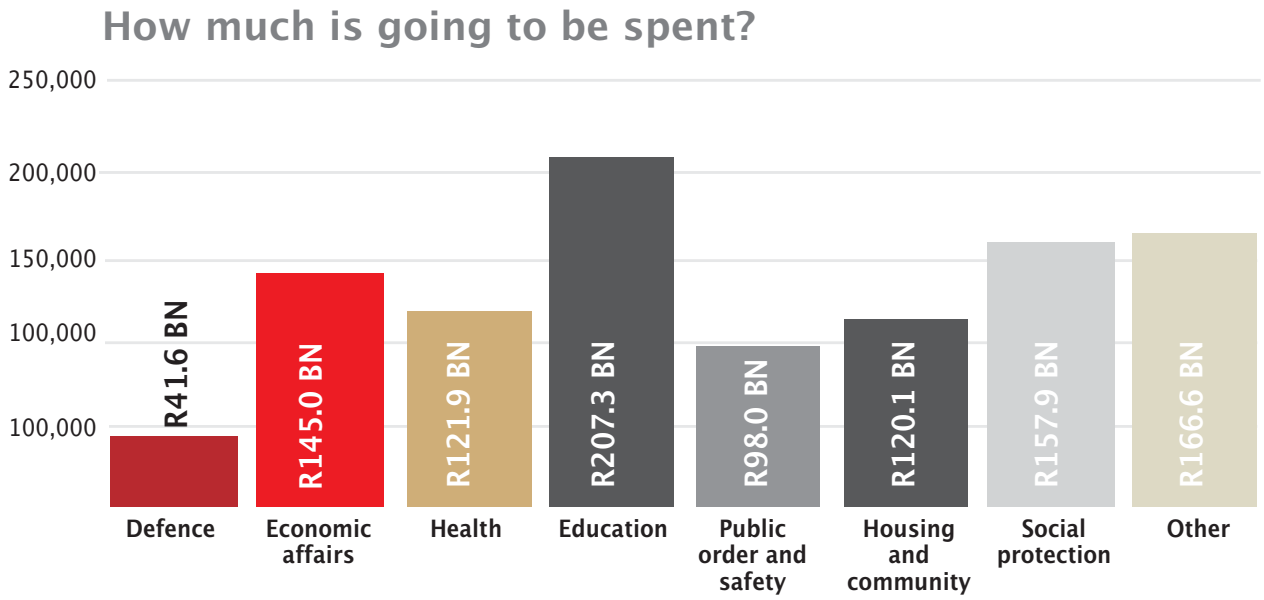
Finance Sector	Government Sector	Telecommunications Sector
During 2012, phishing attacks were on the increase but the associated financial losses decreased. During 2011 there were fewer attacks but the losses were larger. These were not seen as targeted or spear phishing attacks and criminals are still seen to generally use a "shotgun approach" and taking advantage of victims wherever they can Malware infections are also seen to be increasing but we find it also depends on certain popular periods or events during the year Cybercrime is increasing due to the fact that attacks are becoming more and more automated. Criminals now make use of underground services and no longer require in depth technical knowledge The RSA Anti-Phishing service alone recorded a total of 1942 new phishing attacks in South Africa for the first half of 2012	There is a definite increase in the number of stolen credentials such as username and passwords. This is usually done using key logging spy software and recruiting individuals within an organisation to transfer money to bogus accounts Syndicates are placed into organisations to abuse systems. We have seen an increase in foreigners especially targeting specific locals from government to obtain information for them. The local targets may at times be innocent and forced to assist but in most cases are willing participants to partake in the fraud – due mainly to socio-economic circumstances or greed One major government sector said that they see at least 9000 incidents taking place each year Due to thresholds of R100,000 in the Prevention and Combating of Corrupt Activities Act most cases detected are not reported	In the Telecoms sector the number of cybercrime occurrences increased by 200% for 3G data, where criminals are trying to find new mechanisms to get data for free Methods include: • using access network as a LAN • access network (or ftp) to steal virtual vouchers, air time and personal information and • SIM swaps



South Africa's 2012 Budget

To achieve our vision of keeping South African cyberspace a safe place to conduct business and interact socially, will require everybody to work together – government, the private sector and communities.

Government has the lion's share responsibility of dealing with cyber security and cybercrime as they do with any other type of crime or national threat facing the country. They have to invest their limited budgets carefully to meet the demands of the country. Here for example is the South African budget framework highlights for 2012:



Budget Highlights 2102

Spending plans over the next three years

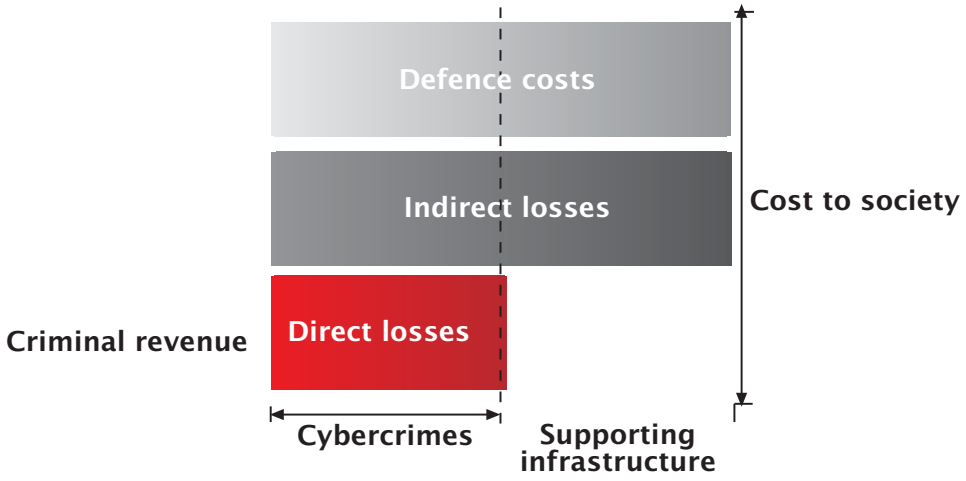
(Source: 2012 SA Budget Highlights – National Treasury)

As countries around the globe scramble to invest in information security, governments want to know that size the investment should be, and what the money should be spent on. This creates a demand among rational policy-makers for accurate statistics of the true cost of cybercrime.

There are many different sources of data on international cybercrime, yet the available local statistics are still insufficient and fragmented; they suffer from under- and over-reporting, depending on who collected them, and the errors may be both intentional (e.g. certain vendors over-exaggerating threats) and unintentional (e.g. sampling bias).

It is therefore important to lay out a framework for analysing the costs of cybercrime.

A Framework for Analysing the Costs of Cybercrime



(Source: Measuring the Cost of Cybercrime – R Anderson)

1 Direct losses

Direct losses is the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime.

Direct loss examples:

- money withdrawn from victim accounts;
- time and effort to reset account credentials (for both banks and consumers);
- distress suffered by victims;
- secondary costs of overdrawn accounts: deferred purchases, inconvenience of not having access to money when needed;
- lost attention and bandwidth caused by spam messages, even if they are not reacted to.

2 Indirect losses

Indirect losses is the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, no matter whether successful or not and independent of a specific instance of that cybercrime. Indirect costs generally cannot be attributed to individual victims.

Indirect loss examples:

- loss of trust in online banking, leading to reduced revenues from electronic transaction;
- fees, and higher costs for maintaining branch staff and cheque clearing facilities;
- missed business opportunity for banks to communicate with their customers by email;
- reduced uptake by citizens of electronic services as a result of lessened trust in online transactions;
- efforts to clean-up PCs infected with the malware for a spam sending botnet.

3 Defence costs

Defence costs are the monetary equivalent of prevention efforts. They include direct defence costs, i.e. the cost of development, deployment and maintenance of prevention measures, as well as indirect defence costs, such as inconvenience and opportunity costs caused by the prevention measures.

Defence costs examples:

- security hardware and software products such as firewalls, antivirus and browser extensions to protect users;
- security services provided to individuals, such as training and awareness measures;
- security services provided to industry, such as website `take-down' services;
- fraud detection, tracking, and recuperation efforts;
- law enforcement;
- the inconvenience of missing an important message falsely classified as spam.

Defence costs, like indirect losses, are largely independent of individual victims. Defences can target the actual crimes or their supporting infrastructure, and the costs can be incurred in anticipation of or reaction to crimes, the latter being to deter copycats.

Total cost to society = (the sum of direct losses + indirect losses + defence costs)

15. What do you believe the financial cost of cybercrime has been to your industry from January 2011 to August 2012?

Commentary

Measuring the cost of cybercrime to the South Africa economy

How much money is currently being lost due to cybercrime each year in South Africa? The answer according to our research is that no-one really knows the total figure for SA. We believe this is due to a number of factors:

- A large percentage of incidents are not being reported to law enforcement or government agencies (see question 22 below for reasons cited)
- Of those cases reported an even smaller percentage of cases actually make it to the courts (where a successful prosecution takes place) and information is then made available to the public domain
- Cybercrime cases are also diluted within common law cases and in most cases prosecuted accordingly as well (due to lax penalties on cyber laws such as the ECT Act versus heavier sentences obtained using common law)
- Lack of cross-industry collaboration and even intelligence sharing across key government agencies once again obscures the true figure.

In an attempt to define an approximate figure for our analysis we have only considered a subset of the direct loss portion and focused solely on the estimated financial theft portion within the three sectors assessed. We calculated the following figures:

Sector value	Theft value in Rands	Theft value in US$ (Based on R8/US$1)	Rationale
Government	R1,5 billion	$187 million	A conservative estimate based on recent incidents and interviews with key stakeholders.
Telecommunications	R1 billion	$125 million	Based on 1% fraud losses (world average is 2%) of combined annual fixed and mobile telephony revenue of R100 billion for SA. (2010 Delta Partners Group)
Finance	R150 million	$18,75 million	Bank customers, according to SABRIC, reported phishing related losses of R92,4 million in approximately 10 000 incidents reported industry wide. A conservative loss estimate based on other known incidents, makes up the balance. With no other reliable industry stats this is considered to be the minimum loss for this sector.
TOTAL direct loss	**R2,65 billion**	**$331 million**	

Note - Based on the government's average recovery rate of 75% and similar case study recoveries, the estimated actual loss figure would be approximately R662,5 million ($82,8 million).

Finance Sector	Government Sector	Telecommunications Sector
Apart from the losses and the clean-up costs of the incident itself, there are hidden costs for prevention mechanisms e.g. purchase of anti-virus software, firewalls, IDS/IPS, subscription to third party reports such as Trusteer, RSA etc The fraud monitoring and detection applications used in SA organisations are not sophisticated enough to sift out specific cybercrime incidents	An estimate of a minimum of R500 million in losses per annum was noted for government. (Actual theft amounts would be around R2 Billion with about 75% of cybercrime related losses being recovered) Government has accumulated a wealth of data relating to the cost of cybercrime in SA but they don't have the analytical resources to accyrately determine what the total figure amounts to 9 out the 43 SA Fraud Prevention Services member organisations achieved a saving of 1.8 Million Rands as a result of losses prevented based on information housed in the SAFPS database	1-2% of the estimated annual turnover of the Telecoms industry is lost through cybercrime and electronic fraud. According to a 2010 Delta Partners Group report the combined fixed and mobile telephony revenue for SA was R100 billion - 1.5% of this figure equates to a possible figure of R1,5 billion Although the rate of cyber attacks in SA is increasing, the lack of visibility into the financial losses incurred is alarming. This furthermore results in an unbalanced security focus and protection against unrealistic security threats The cost for defensive cybercrime

Finance Sector	Government Sector	Telecommunications Sector
	The Protective Registration service has more than 16 000 listings for individuals whose ID's have been lost, stolen or used fraudulently. Between 2009 and 2011, 5940 individuals were recorded as victims of impersonation on the SAFPS database which serves to prove that we are not immune from this threat in South Africa	measures is around R25-30 million and is increasing due to rising mobile cybercriminal activity

Perspective: The true cost of cybercrime – robbing innocent children or future home-owners:

The Department of Social Development will receive an additional R1.4 billion over the next three years to increase access to early child development for an additional 80 000 children and to roll out an in-house and community based childcare and protection programme (Isibindi). The Isibindi project will benefit 858 000 children and adolescents, with a focus on rural communities, orphans and child-headed households. About 10 000 youth workers will be employed in this programme.

If we therefore consider the potential R662,5 million cybercrime loss above to be close to 50% of the Isibindi programme above, cybercriminals are in essence robbing 40 000 children of a childcare protection programme and 5 000 youth workers from gaining employment.

It is said the average cost of a Reconstruction and Development Programme (RDP) low-cost house is R65,000. The potential R662,5 million cybercrime loss above would therefore rob over 10,000 underprivileged families from receiving much needed shelter.

This is the true cost of cybercrime to our country!

16. Do you believe your industry + SA as a whole is investing enough resources to sufficiently mitigate the threat of cybercrime?

With the significant increase in the use of online and mobile channels, increased compliance requirements and a stronger governance focus more resources have been allocated to fighting crime. The question to ask however is, have similar investments been made in the cybercrime and information security sectors?

This involves investing in better frameworks and processes for communicating vulnerability and threat information – a common platform to share intelligence dynamically with key stakeholders.

Finance Sector	Government Sector	Telecommunications Sector
Individual companies are investing resources to deal with the issues directly affecting them. However, cybercrime is not getting dealt with sufficiently on a national level. For example – criminals move from one bank to the next one as the banks increase their security. Nothing is done to completely eliminate the threat This depends on the risk appetite of organisations as the biggest obstacles are often obtaining training budgets	I think they are investing adequately to the extent of the problem and the needs of the current South African society. A more simple and main media (TV and radio) awareness campaign may improve awareness levels. In short there is no perceived crisis arising from cybercrime in this country but there is a need for skills development Cybercrime is not the biggest issue in SA right now, but it is growing. We need to invest NOW so in 5yrs we will then have the skills / resources to deal with	Not enough is invested as this is NOT the primary focus. Our main challenge is to compete in this space with increasingly less people, less budget and cost cutting Industry tends to treat security as an add-on fix for audits lacking focus of real security value and requirements Electronic identity theft is not just a hype it is a real thing in this country. SA organisations are losing a lot of intellectual property and not enough is

Finance Sector	Government Sector	Telecommunications Sector
Banks are spending a large amount of money as this is a higher priority for them. However more research still needs to be done in order to understand the current SA situation and where further investments should be made Law enforcement needs to create more technological capacity to investigate and prosecute as crime trends follow business trends – more crimes are being perpetrating using electronic devices or platforms	the growing threat of cybercrime. Building skills to build future capability today SA does not have enough skilled resources with knowledge on investigation and digital forensics, identity fraud and data fraud Similar to a serious wound that is being treated with healing plasters over and over again, we don't look at the root cause and fix the problem. In most cases the root causes are the socio-economic challenges of this country Expert pools should be established to ensure end-to-end coverage SA does not invest enough resources because this is a costly exercise. Approximately close to a million rand per person is needed to train an entry level person on digital forensics	being done in SA Based on the number of occurrences and financial losses not enough is being invested in SA SA needs more focus overall around detection and data visibility, to build monitoring and detection systems for all systems from inception and the visibility of data is of utmost importance

17. Does your organisation/industry receive sufficient training in the area of cybercrime management? What type of training is needed for your industry and SA?

Commentary

Despite the local shortage of skilled information security professionals there is still insufficient deep technical training done in South Africa. More structured training and education needs to be incorporated at the SA university level as modules in degrees.

Efforts to enable judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence through training, networking and specialisation are on-going and there is a project of cybercrime for judges currently funded by contributions from the Government of Romania, Microsoft and McAfee (through the Silicon Valley Community Foundation) which complement Council of Europe funding.

Finance Sector	Government Sector	Telecommunications Sector
SA needs more investigative and prosecutorial skills Recruitment within SAPS is also not done correctly. The right people with the right skills are not always recruited for cyber related jobs and are used on other cases because of the volume of other crime cases. Hence cybercrime cases don't get enough focus and resources aren't getting enough experience. SAPS entry level recruits don't get trained on how to deal with cybercrime incidents or with opening up a cybercrime docket	SA needs regular discussions on cloud security, networks and new technologies to educate people Digital forensics and investigative skills are in need. Some organisations rely on SABRIC for this There is a requirement to be properly defined according to business and technology environments. Specialist teams to be compiled combining business, technology, security, forensic and investigative expertise	Cyber security skills are developed on the job. There is generally very limited security training due to cost and a security resource limitation Cyber training should be developed by information security industry to support South Africa in cyber-attack awareness and general security domain knowledge Expertise is required across a spread of business & business systems, underlying technology landscape, security analytical, forensic and investigative skills

Finance Sector	Government Sector	Telecommunications Sector
The biggest problem is to change the mindset within law enforcement in general regarding cybercrime issues. There is not enough insight at present to realise that cybercrime related issues are a current threat and will be for the longer term and that capacity and skills to deal with it, is no longer optional SA does not have a sustainable model for development of resources with the right skills Basic training should expose entry level policeman to the subject matter experts	in accordance with problem areas Expertise is required across a spread of business & business systems, underlying technology landscape, security analytical, forensic and investigative skills We can't train people if we don't know what skills we need and at what level hence research needs to be done in this area Digital Forensics used in the government area has no ongoing training programme – the methodology used is outdated SAPS have up to a 3 year backlog and a shortage of resources. Private sector has offered free tools / training/ resources to government but government don't take this offer up and are afraid of being exposed We need proper cyber forensics core skills and not just training on a specific tool Insufficient training but growing in terms of SANS coming to SA Requirements to be properly defined according to business and technology environments. Specialist teams to be compiled combining business, technology, security, forensic and investigative expertise in accordance with problem areas	

18. What emerging threats or other significant cybercrime risks are being encountered by your industry?

Emerging information exchange and access channels such as mobile and cloud technologies are providing new targets to an increasingly professionalised industry of cyber criminals. This trend is exacerbated by Bring your Own Device (BYOD), which exposes the resources of organisations whose employees use their personal (and often unsecured) devices to access organisational information.

Finance Sector	Government Sector	Telecommunications Sector
Banks are seeing the same common vulnerabilities being exploited. Very rarely do we see anything different however we need to be prepared for the range of more sophisticated attacks when they do occur The threat of staff members being targeted by external syndicates is still a huge problem in SA. End users are being targeted either through bribing or intimidation to infiltrate systems/machines e.g. installing keyloggers	The prevalence of cybercrime attempts are increasing. The sophistication is the same i.e. in the main the crime is a copy of what is already out there in the global world. Keyloggers are still a problem today in SA Threats include victim impersonation and identity theft The ECAC has identified that the most pressing technology constraints facing law enforcement agencies at present are	Targeted attacks are becoming more frequent, thought out and sophisticated with the aid of external syndicates using USB or PSP keyloggers and some with SIM capability Emerging threats include session high jacking of VoIP sessions, exploration of customer, private and financial information Phishing attacks are getting smarter Using technology to aid in the crime

Finance Sector	Government Sector	Telecommunications Sector
Other threats include tampering with point of sale devices and card reading devices being compromised before shipment to customers Remote access to systems, BYOD and security surrounding cloud computing are also major factors	the challenges presented by criminals using 3G internet access and the inability to properly track certain internet browser IP addresses	process – e.g encryption Mobile and Social media avenues will increase

19. Do you believe that the creation of an independent (non-government) organisation with the aim of assisting SA companies to report cyber threats to a central point that will provide incident management assistance, streamline reporting to law enforcement, provide an early warning system to the community and generate relevant stats would make the fight against cybercrime more effective? How do you see this model working?

South Africa needs an independent body that will collate information regarding incidents and trends from various sources to indicate what vulnerabilities and threats are prominent, what attack types have been successful, trends and incidents related to mobile technology, social media and global, African and local information security trends.

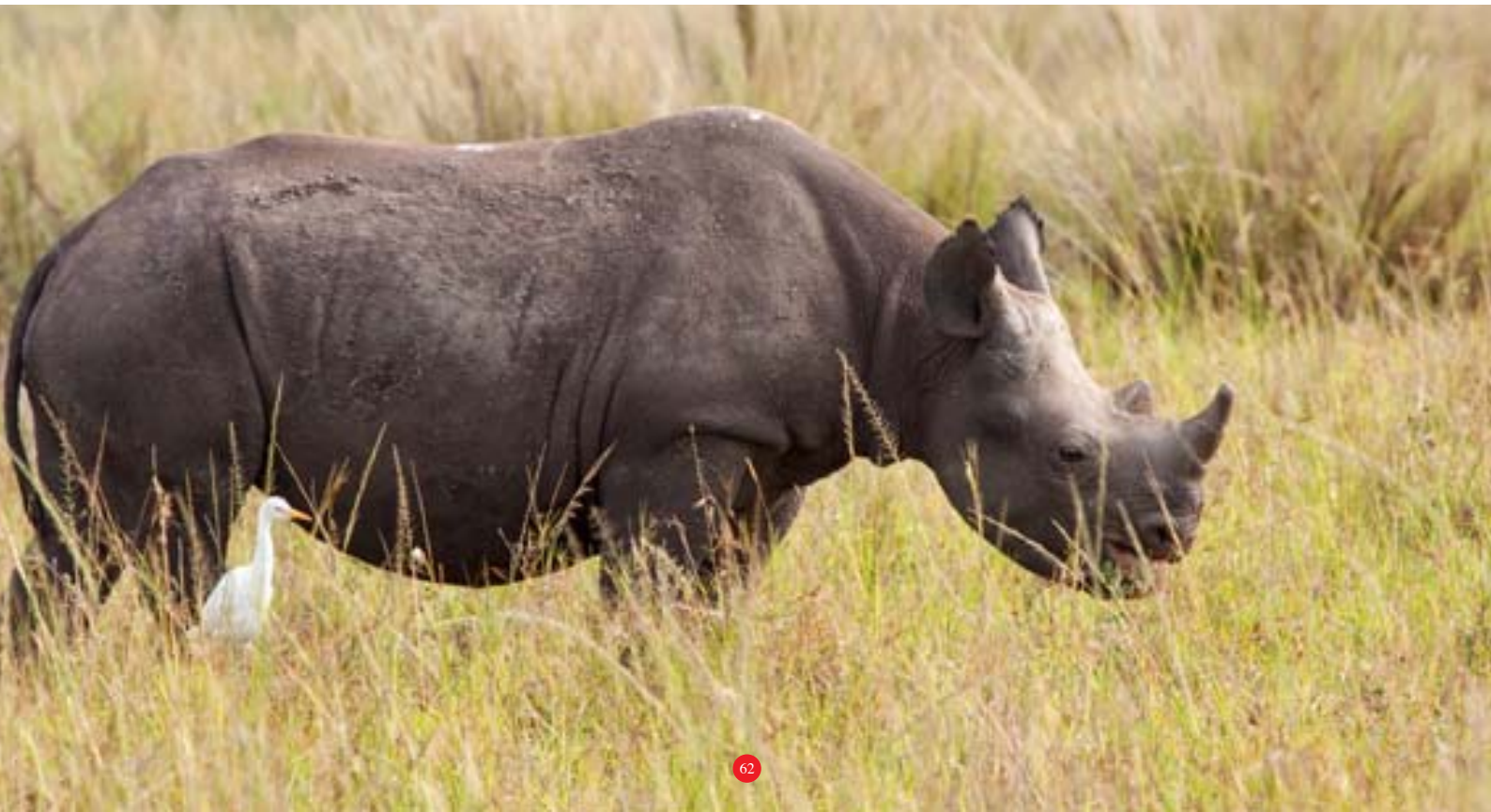
Finance Sector	Government Sector	Telecommunications Sector
Sector CSIRTs owned by the sector/industry work better, more effective. However these sector CSIRTs need to communicate with each other. People in a similar industry tend to know each other better, establish trust and can share knowledge. Sharing of information is crucial. Sending general information to crime intelligence agencies will be useful. This could be used to receive updates and reports The Banking CSIRT (via SABRIC) is currently doing this and their model works. There is a trust established. SABRIC banking CSIRT aims to partner not only with the banking sector, but also telecoms and ISPs as stakeholders (not members) once they have similar structures up and running The SABRIC banking CSIRT will align with the National CSIRT – they have the mandate to contribute to fighting cybercrime at national level	A holistic model driven by government and private sectors including law enforcement is needed. Security cluster departments from Intelligence to police to prosecutors must work together to understand how the process works The central point should have sufficient expertise to guide the incoming channels and sources to recommend and facilitate the appropriate course of action. Client organisations should channel all issues via a specific office. Various scenarios should be mapped with workflow of reporting and activities as guidelines of how it all fits together in order for organisations to get a feel of what to expect. Such a model will also allow constant improvement in the structure, activities and reporting This can work but must function as a CSIRT. In the absence of a CSIRT this is crucial to pool intelligence, sharing of information and to provide support and guidance	A National CSIRT will only work if there is a good relationship and integration into government Yes – but will take time for broad adoption Various scenarios should be mapped with workflow of reporting and activities as guidelines of how it all fits together in order for organisations to get a feel of what to expect. Such a model will also allow constant improvement in the structure, activities and reporting

20. Does your organisation or industry participate in public-private partnerships for prevention and combating of cybercrime? What initiatives are currently taking place?

Commentary

One of the best ways to counteract the flow of information across the global cybercrime economy is cross-industry, public-private collaboration on a global scale.

Finance Sector	Government Sector	Telecommunications Sector
The Banking CSIRT coordinated by SABRIC is currently underway Banks are planning Digital Analysis Centre for intelligence purposes Anti-Phishing group Inter-bank electronic banking crime workgroup has been operational for many years and comprises banks, law enforcement as well as stakeholders from other industries SABRIC also runs a crime awareness campaign at an inter-bank level	We need to get the right parties involved, first at a regional level and then at an African level. We need to pool efforts together and openly share information and experience The SA Cyber Security Academic Alliance is an initiate between 3 universities - UJ, UNISA and NMMU	A lot of it is project based with various inter-agency committees as well as external bodies. In general there is an agreement to establish partnerships. Still very contained at present



21. What partnerships should be developed on a National, African or International level that would add value to SA?

Commentary

Government cannot combat crime alone and key partnerships across multi-industries in SA, the African continent as well as Internationally are vital to our country's success going forward.

Finance Sector	Government Sector	Telecommunications Sector
International organisations don't have a CSIRT in SA to contact. A national central point to give advice would be very effective and would also be able to interact with similar structures globally. Collaboration is important but the benefit and roles/responsibilities must be understood to a network must be formed South Africa should become more involved in international collaboration efforts South Africa needs to ratify the cybercrime treaty to avoid becoming an easy target for international cybercrime	South Africa is at the core of partnerships at an international level. There is a need however for partnerships at a national level between the private sector, individuals, civil Society and government. Such partnership must serve a national need in support of government efforts A number of cybercrimes are borderless and unless we combine efforts with other countries we will never catch the bad guy. Hence SA needs to ratify the Budapest Convention on Cybercrime and be actively involved in all African Union cybercrime initiatives SA needs to form partnerships with international fraud prevention bodies such as CIFAS	Partnerships in the telecommunications industry is a challenge due to industry regulatory and legislation restrictions. We believe that a cross industry platform can be the only successful model to start from where after it could mature to industry specific partnerships It would be good to have more International and African collaboration but we need to get it right for SA first SAPS don't have the resources to investigate and prosecute effectively – more ebusiness and ecrime type partnerships are needed

22. What do you believe are the most significant reasons that organisations sometimes do not report cybercrime incidents?

Commentary

An organisation's failure to report cybercrime is typically rooted in the concern that their brand or business will suffer negative consequences if news of the crime were to leak out.

Customers and other stakeholders would normally forgive a once-off incident occurring but not tolerate an organisation that continuously failed to implement the necessary security controls.

Finance Sector	Government Sector	Telecommunications Sector
Loss of customers Credibility Reputational risk Lack of confidence in law enforcement Organisations don't know who to trust or who to report incidents to It is easier to deal with the issues ourselves as opposed to dealing with government agencies	Reputational risk is the primary reason There is no law that forces organisations to report the incident - they DON'T have to report the incident Fear of damage of reputation, fear of opening a can of worms No confidence in SAPS capability to resolving cases Loss of reputation / trust Avoid potential action against organisation Avoid exposure of lack of sufficient controls and compliance	Inability to prosecute or understand the issues Brand reputation Loss of faith in law enforcement system Protection of reputation and revenue Government resources are limited and not adequately skilled Small organisations do not have any place to report cybercrime or get support Organisations don't believe that anyone can do anything about it and a fair amount of apathy exists

23. In your experience over the last 3 years when cybercrime incidents are reported to law enforcement what type of response did you receive?

Finance Sector	Government Sector	Telecommunications Sector
If the cybercrime charge is reported at the station level - there is a lack of understanding as what to do If the cybercrime charge is reported at the DPCI / commercial branches there is a better response and capacity is being created to deal with the complaints effectively. However, there is a noticeable progress in recent years with law enforcement acknowledging that they need to prioritise and address the threat In general local police stations lack skills and experience in opening cybercrime dockets	The principle of law enforcement agencies is that cybercrime is similar to any other crime depending on the numbers involved. The SAPS runs a fulltime cybercrime unit that works very well with the fraud unit. They also view most of the cybercrime as white collar crime. The response has improved significantly in the past two years and co-operation with banks added to the improvements All cybercrime related incidents go to the commercial detective department at SAPS. Unless the incident is over R100 000 nothing is done about it. The current situation is not improving. There is definitely a serious lack of skills and resources at SAPS	Other than recording the docket sometimes there is no response from law enforcement. No real investigations are conducted The support is actually deteriorating not only from law enforcement but also from industry where individuals who have suffered a loss as a result of cybercrime are increasingly left on their own to deal with their loss The technical system intrusion cases are generally too complex and are not dealt with. Based on this country's socio-economic situation cybercrime is a low priority and not being dealt with affectively

24. Based on your knowledge, do organisations make use of in-house staff or external service providers if conducting their own investigations into a cybercrime incident?

Finance Sector	Government Sector	Telecommunications Sector
Technical malware analysis might be outsourced however the investigative work remains in-house Banking industry mostly conducts their own investigations and where appropriate may contract expertise in They have specialised investigators who are also responsible to recommend changes where system or procedural short comings have been noted Cases are also reported to SAPS who then do criminal investigations supported by the banks and SABRIC The industry works with the commercial branches within the DPCI as well as the SCCU's where the value of the case meets their criteria or the matters are deemed to be complex	Investigations are conducted both in-house and external service providers are also used, depending on the nature and complexity of the incident and skills required There is also collusion between fraud syndicates and in-house staff who are used as "mules". When we suspect internal collusion then we may also bring in outside help to perform a sting operation	Investigations are mainly conducted in-house for general planning and handling of incidents but external specialists are used in larger cases and when cloning of hard drives is required. There is however an increase in deployment of fraud detection and prevention technology internally

25. To what extent are the findings from any investigation into a cybercrime incident used to improve the information security in an organisation?

Finance Sector	Government Sector	Telecommunications Sector
Findings are used all the time to learn from and improve the current security position. The banking industry is very good at using lessons learnt to prevent further incidents. The culture of lessons learnt is well institutionalised Past information is crucial in understanding what to do when a cyber attack occurs and how to resolve it or prevent it From a banking perspective lessons learnt are used to improve security such as chip cards, SMS alerts and OTP's created in the banking environment	In most instances the recommendations identified from the incident report are usually implemented immediately. The incidents usually get the attention of senior management who want recommendations implemented to avoid future occurrences Findings can lead to vulnerabilities discovered and mitigated, strategic intervention depending on complexity, improved awareness and education – thus overall better level of security maturity In some government sectors this is not being done and we need an organised way of doing this. This must become a priority	This is highly dependent on the organisation itself. Ideally vulnerabilities exposed by a cybercrime incident would be addressed immediately and effectively. However identifying the vulnerability may itself require a forensic investigation that not all organizations have the financial or personnel resources to utilise Lessons learnt are used by the fraud department and in most cases only if the exposure was of a sever nature causing the company substantial financial loss

26. Do you believe that our current legal framework is sufficient to assist with the apprehension and prosecution of cybercriminals?

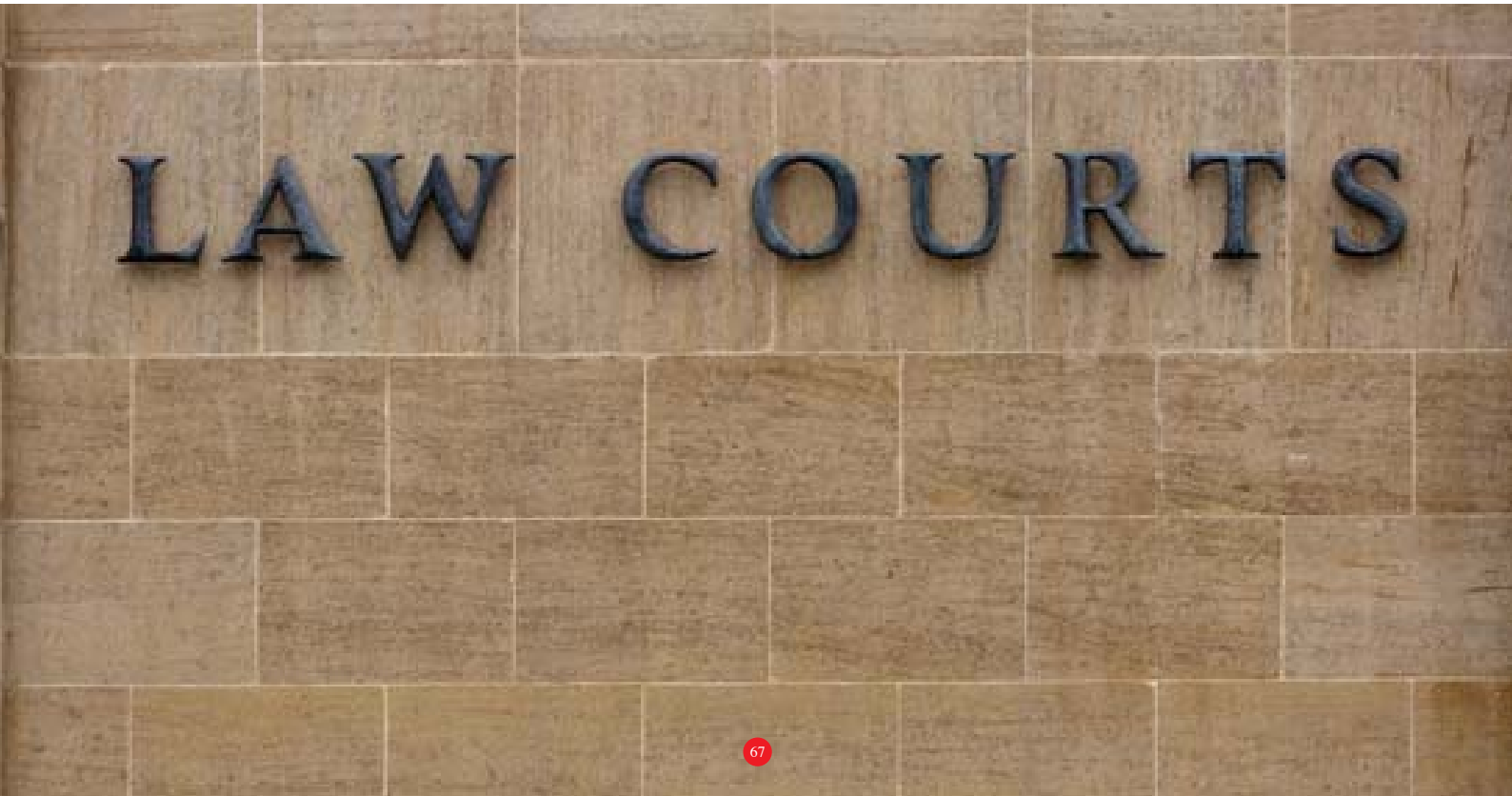
Considering SA's position as a developing country, our regulatory and legislative framework for information security compares well against other developing countries. However, the implementation of good practice is still lagging, especially in the small to medium sector space.

As South Africa is a late-adopter, there will be the benefit of hindsight from other international attempts that may aid in the introduction of a strong legal framework; however, it is essential to introduce a strong technical framework to support it. These frameworks will provide the mechanisms with which to protect South Africa's infrastructure.

Finance Sector	Government Sector	Telecommunications Sector
There are laws and regulations in place however the investigative aspect is lacking with a shortage of law enforcement and legal resources and skills The ECT act is in place but the penalties are not harsh enough The courts are still battling to understand and prosecute frauds where a computer was used as an instrument There should be more legal expertise including expertise of judges on the subject of cybercrime	Currently there is no legislation specifically applicable to cybercrime and it is treated like any other crime. There is a need for legislation with minimum sentences for different types of cybercrimes. It is also encouraging that there is a team already drafting this legislation within the JCPS cluster There is a higher prosecution sentence using RICA. RICA has been used to prosecute against spyware. Most cybercrime related cases are prosecuted using other legislation such as the common law act and categorised as either fraud or theft. There have been cases prosecuted using Section 86.1 of the ECT act, however these were minor incidents where a maximum penalty of 12 months. There are no laws to prosecute against identity theft	The ECT ACT needs to be updated with more relevant cybercrime issues There is a lack of skill to deal with cybercrime issues and the penalty for ECT Act is so low that these crimes are categorised as other types of fraud With the implementation of the PoPI Act it will be important to get better prosecutions as the act forces companies to disclose incidents Our cybercrime laws are sufficient – section 86, 87,88 of the ECT Act provide a fairly good framework. The bigger problem is with the actual prosecution process

27. According to the Electronic Communications and Transactions Act, 2002 (ECT act), the penalty of a fine or a maximum of 12 months imprisonment has been criticised as being too lenient. What is your view regarding this?

Finance Sector	Government Sector	Telecommunications Sector
The penalties are too lenient and not a deterrent at all. The real problem is that the justice system is not geared to handle enough convictions The current penalty is not a deterrent at all The ECT act had a different focus when it was released over a decade ago and was more focused on the proper use of ICT. In short there is a need for a complete rethink of the act with a special focus on cybercrime	The activities that the ECT act lays out penalties for (e.g. spamming, sending viruses) have extremely high financial and personal consequences worldwide – global cybercrime losses have been estimated to exceed $114 billion annually . The penalty for any offense should be weighed against the consequences as well as the intention. With this in mind the ECT act penalties are not stringent enough to act as a deterrent The ECT act is outdated and needs to reflect current issues specifically regarding cybercrime	The impact of the crime on society cannot be adequately assessed due to the fact that the lack of lawful prosecution and assessing do not identify all the other incidents that were perpetrated by the attacker The penalties are not harsh enough Sentences are way too lenient – that's why prosecutors don't report it as cybercrime (section 86,87,88 in ECT act) Common law offensive crimes have better penalties and this is often used to sentence cybercriminals



28. What is your perception of the capability of the National Prosecuting Authority (NPA) to prosecute cybercrimes in SA?

Finance Sector	Government Sector	Telecommunications Sector
Prosecutors and judges are not skilled enough to understand cybercrime issues. We need more specialised units for cybercrime SABRIC provides assistance to law enforcement in this area as well as it is a specialised area Some of the issues the victims of cybercrime have with the justice systems are: • They don't trust police and don't have any faith that anything will be done if they do report it • They don't want to spend even more of their time filling out forms and talking to law enforcement personnel and generally dealing with the "hassle factor" involved in reporting • They don't think the crime is significant enough or their losses large enough to warrant taking up the time of law enforcement • Or simply, they just don't know where to report due to lack of awareness	This is a global problem and prosecuting such crimes is a challenge for most countries in the world. Prosecutors, defence lawyers and judges need special programmes on ICT law The NPA has the capability but require continuous efforts to stay abreast of new threats and technologies There are lots of incidents that could be potential cybercrime incidents but they are not being prosecuted. Law enforcement is under severe constraints regarding resources and lack of skilled people and experience We have room for improvement by understanding what the current cybercrime situation is in SA, assessing what is needed to improve and implementing metrics to get it done	Our perception is that they are not prosecuting much as media visibility is low There is definitely a shortage of skills and we need to invest in aggressive training and significant amendments to the legal framework We need more media awareness of prosecution cases to send out a strong message to criminals We need more specialised courts The volume of prosecuted cases are currently low hence the lack of prosecution skills

29. How many cases in your industry do you know of where a cybercrime prosecution took place?

Finance Sector	Government Sector	Telecommunications Sector
There have been several cases – with Postbank being a recent example Judgments on cases involving cybercrime in South Africa reported by the media are dominantly on the evidence provided through usage on digital and internet applications like email, SMS and video captured through mobile phones rather than conviction of cybercriminals who used methods like phishing, smishing or botnets Most of the Cybercrime provisions in the ECT act are noble endeavors; however their enforceability is still to be tested in South African Courts	The NPA only see the cases that are handed over by SAPS. Less than 5% make it to court and are categorised as cybercrime. There has been no denial of service (DOS) or botnet prosecution. The NPA is called unofficially for advice but don't receive that many cases for prosecution SA needs more specialised teams to assist with the investigation so that cases are brought forward for prosecution There are lots of cases prosecuted using Section 86.1 of the ECT act, however these are minor incidents where a penalty of max 12months is sufficient. The problem is not the convictions, it's the penalty	Many cases are pending, but none that have been prosecuted. We also feel that penalties are not harsh enough, especially in relation to statutory offences of the ECT Act

30. What local initiatives are currently underway to improve SA's existing cybercrime legal framework?

Finance Sector	Government Sector	Telecommunications Sector
We need initiatives with the support of both government and the private sector to train all relevant people dealing with cybercrime from investigators to prosecutors We need to train our local police team from the entry level police constables basic cybercrime skills such as how to identify, categorise and open a docket for cybercrime incidents	A Parliamentary Standing Committee for Cyber Security Oversight The state is currently working on a full review of cyber security focusing on cybercrime, information security, national security, e-Identity and many others	We need to build a trusted community and have regular, ongoing meetings to pool information and share experiences

CONCLUSION

Our economic growth depends on attracting new business and this implies a stable e-infrastructure: network bandwidth, resilience and the ability to respond to cyber incidents within hours rather than days or weeks.

South Africa has the opportunity to become the leading nation on the continent in terms of information security innovation. The apparent strategic lack of focus on information security priorities (in particular cyber-security and cybercrime arenas) may eventually hinder economic development due to direct financial losses from cybercrime and loss of confidence of local and foreign investors.

With tighter local and international legislation on the horizon South African companies may also be unable to meet the costs and complexities associated with compliance.

The introduction of a national CSIRT will assist organisations with incident management and provide much needed intelligence regarding the threat horizon facing South Africa. Such a facility would also provide crucial support and coordination in the event of increased cyber-attacks against the countrys resources.

Raising awareness and implementing specialist information security training programmes will greatly improve the nation's vulnerability to cyber threats.

All these initiatives are beneficial to South Africa but they do come at a cost. Will this cost outweigh the benefits of establishing a secure and stable digital environment in SA?
We hope that this report provides a credible input to the leaders that have to make the tough decisions on our behalf. Our opinion is that it is worth making the investment now to prevent far greater losses in the near-future.

We intend conducting yearly SA Cyber Threat Barometer projects to monitor progress and assist our country with obtaining the optimal return on investment. We furthermore wish to expand our project scope to include additional African countries.

References

Reports

Bay, A. (2011, Januray 18). Tunisia's Remarkable Revolt. Retrieved January 19, 2011, from Strategy Page On Point Blog: http://www.strategypage.com/on_point/20110118224752.aspx

Bronstein, P. (2010, April 6). The Wikileaks Incident: How Social Media has Change Warfare Coverage. Retrieved April 7, 2010, from The Huffington Post: http://www.huffingtonpost.com/phil-bronstein/the-wikileaks-incident-ho_b_527788.html

CERT Brazil. (2011). CERT.br Stats. Retrieved August 26, 2011, from CERT.br: http://www.cert.br/stats/incidentes/

CERT-Africa. (2010a). CERT in Africa. Retrieved May 3, 2010, from: http://www.cert-africa.org/node/3 CERT-Africa. (2010b). Morocco to establish MA-CERT. Retrieved May 3, 2010, from: http://www.cert-africa.org/node/135

Cisco. (2011). Cisco 2010 Annual Security Report. Retrieved January 24, 2011, from Cisco Security Reports: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf

Couzyn, Hertzog & Horak, Cyber Crime In South Africa, July 30, 2008
Gendarmerie Nationale 2011 – Prospective Analysis on Trends in Cybercrime from 2011 to 2020,

Eric Agwe-Mbarika Akuta, Isaac Monari Ong'oa, Chanika Renee Jones Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice, 05 April 2011

Grobler, M., Jansen van Vuuren, J., & Zaaiman, J. (2011). Evaluating Cyber Security Awareness in South Africa. Proceedings of the 10th European Conference in Information Warfare and Security (pp. 113-121). Tallinn, Estonia: Academic Publishing.

Group-IB's CERT-GIB analysts --- State and Trends of the Russian Digital Crime Market 2011

Indian CERT. (2011). Annual Report. Retrieved August 26, 2011, from CERT-In: http://www.cert-in.org.in/

International Telecommunications Union. (2011, May 23). ICT Data and Statistics. Retrieved May 31, 2011, from:www.ITU.int: http://www.itu.int/ITU-D/ict/statistics/index.html

Internet Crime Complaint Center. (2011). 2010 Internet Crime Report. Retrieved August 24, 2011, from IC3 Annual Reports: http://www.ic3.gov/media/annualreports.aspx
Adv Jacqueline Fick, Pwc Southern Africa, Cyber Crime In South Africa: Investigating And Prosecuting Cyber Crime And The Benefits Of Public-Private Partnerships, March 2009
Dr Khomotso Kganyago- Information Security Discussion by Microsoft South Africa's Chief Security Advisor, Cybersecurity Agenda – How are we doing in South Africa?

Kristina Cole, Marshini Chetty,Christopher LaRosa, Frank Rietta,Danika K. Schmitt,
Seymour E. Goodman, Cybersecurity in Africa: An Assessment, 2008

Leyden, J. (2011, February 7). NASDAQ Admits Hackers Planted Malware on Web Portal. Retrieved August 12, 2011, from The Register: http://www.theregister.co.uk/2011/02/07/nasdaq_malware_breach/

Microsoft Corporation. (2011a). Microsoft Security Intelligence Report, vol. 10. Retrieved May 4, 2011, from: http://www.microsoft.com/security/sir/archive/default.aspx Microsoft Corporation. (2011b). Microsoft Security Intelligence Report - Global Threat Assessments, vol. 10. Retrieved May 4, 2011, from: http://www.microsoft.com/security/sir/default.aspx

Microsoft Security Intelligence Report, Volume 12, July through December, 2011

Mills, E. (2011, April 18). Cyber Attakcs Rise at Critical Infrastructure Firms. Retrieved May 13, 2011, from CNet News: http://news.cnet.com/8301-27080_3-20055091-245.html?tag=mncol;mlt_related

Pl Yong, New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime, December 2011, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/Cyber_cp_china_Pi_Yong_Dec11.pdf

Proceedings of the First IFIP TC9 / TC11 Southern African Cyber Security Awareness Workshop 2011

Richard Boateng_ Olumide Longe, Victor Mbarika, Innocent Avevor, Stephen Robert Isabalija, Cyber Crime and Criminality in Ghana: Its Forms and Implications,Year 2010

Rita Tehan Information Research Specialist, Cybersecurity: Authoritative Reports and Resources, July 3, 2012
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Song, S. (2011). African Undersea Cables. Retrieved August 24, 2011, from Many Possibilities: http://manypossibilities.net/african-undersea-cables/ South African Cities Network. (2011a). Retrieved May 20, 2011, from: http://www.sacities.net/ South African Cities Network. (2011b). State of the Cities Report. Retrieved May 30, 2011, from http://www.sacities.net/what/strategy/report/607-towards-resilient-citie

Southern Africa: Region Cracks Down on Cyber Crime, BY KIZITO SIKUKA, 12 APRIL 2012, http://allafrica.com/stories/201204120866.html

Symantec Corporation. (2011a). Symantec Internet Security Threat Report, Vol. 17: Trends for 2012, from: http://www.symantec.com/business/threatreport/

Symantec Corporation. (2011b). Norton Cybercrime Report 2011. Retrieved September 21, 2011, from Norton South Africa: http://za.norton.com/content/en/za/home_homeoffice/html/cybercrimereport/#nav

Trustwave. (2011, January 19). Global Security Report 2011. Retrieved February 3, 2011, from Trustwave Global Security Report: https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2011.pdf

Van Niekerk, B. (2011). Vulnerability Assessment Of Modern Ict Infrastructure From An Information Warfare Perspective

Verizon Risk Team, 2012 Data Breach Investigations Report

Website URLs

http://www.csir.co.za/dpss/docs/SACSAWFinal_16Aug.pdf
http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR03523:@@@D&summ2=m&
https://www.eff.org/deeplinks/2012/08/victory-over-cyber-spying
http://www.whitehouse.gov/administration/eop/nsc/cybersecurity
http://www.nbcwashington.com/news/tech/UMd-Northrop-Grumman-Develop-Cybersecurity-Partnership-158449925.html
http://www.marketwatch.com/story/umd-and-sourcefire-announce-new-cybersecurity-partnership-2012-07-12
http://www.insaonline.org/index.php?id=79
http://www.cyberpartnership.org/about-overview.html
http://www.gao.gov/products/GAO-12-876T
http://www.cabinetoffice.gov.uk/resource-library/us-uk-cyber-communique
http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf
http://www.cabinetoffice.gov.uk/reports/national_security.aspx
http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx
http://www.i-policy.org/2012/02/brazil-draft-cybercrimes-law.html), http://www2.camara.gov.br
http://www.digitaltrends.com/web/beyond-cispa-the-cybersecurity-bills-you-need-to-worry-about-right-now-cybersecurity-act-of-2012-secure-it-act/#ixzz22anScCLy
http://www.cg.org.br/
http://www.nbso.nic.br/
http://www.nbso.nic.br/contact-br.html
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus2012/presentations/Update_Grudinov_IB.pdf
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus2012/presentations/Update_Grudinov_IB.pdf
http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf
http://www.css.ethz.ch/publications/pdfs/RAD-62.pdf
http://www.scribd.com/Silendo/d/80154379-SDA-Cyber-Security-The-Vexed-Question-of-Global-Rules
http://mit.gov.in/content/cyber-security-strategy/
http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf
http://www.asianlaws.org/brochures/cyber-law-police-brochure.pdf
http://www.slideshare.net/nicolascaproni/an-investigation-into-chinese-cybercrime
http://news.hostexploit.com/cybercrime-news/4742-china-lost-3-billion-to-cybercrime-in-2010.html
http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794
http://www.sans.org/cyber-guardian/
http://csrc.nist.gov/nice/framework/documents/national_cybersecurity_workforce_framework_printable.pdf
http://www.csoonline.com/article/221695/red-team-versus-blue-team-how-to-run-an-effective-simulation
http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm
http://hackmageddon.com/
http://www.microsoft.com/security/sir/threat/default.
http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf
http://www.faronics.com/2011/7-types-of-cyber-criminals/
http://www.londonactionplan.org/
http://www.paladion.net/phishing/index.html

One strong wolf alone cannot defeat a pack of dogs (Chinese proverb)

To effectively manage risk in your IT Governance, Privacy or Information Security Programme you need great people on your team. We help companies optimise their valuable people assets through:

- Mentorship
- Research
- Training & awareness
- Toolkits & simulations

WOLF PACK

www.wolfpackrisk.com