Why is a secure Cyber Space essential to South Africa?

Prof Basie Von Solms
Director : Centre for Cyber Security
University of Johannesburg
basievs@uj.ac.za
Main purpose of this discussion

• To revisit with you as important stakeholders and users of Cyber space a number of aspects related to Cyber Space

• Re-iterate our dependence on Cyber Space

• Debate the possibility of securing Cyber Space

• Debate the role the different stakeholders to secure SA’s Cyber Space and evaluate the present position
What is Cyber Space?

• All computers, computing devices, phones, users etc using the Internet

• Cyberspace is today the fifth domain of human activity, in addition to land, sea, air and outer space.

• Our dependence upon cyberspace for social, economic, governance, and security functions has also grown exponentially
Cyber Space

- Authorised students, staff etc
  - Library Databases
  - Financial Databases
  - Student Databases
  - HR Databases

- Un-authorised Users

Internet

USERS

Cyber Space
Threats

- Identity theft
- Masquerading
- Interception
- Unauthorised access
Our daily lives are progressively integrated with Cyber Space

Examples of such environments are:

- The Financial Environment (Internet banking)
- The Health Environment
- The Power and Electricity environment
- The Fuel Provision and Distribution environment
- The Travel environment (Air, Sea etc)
- The Sanitation (sewerage) environment
- The Food Supply environment, including food production and food distribution
Our daily lives are progressively integrated with Cyber Space (cont ..)

Examples of such environments are:

- The Government Services environment for serving citizens
- The Telecommunications environment
- Internet of Things
- Social networking
- and many more.
Let us investigate some of these environments in more detail
Financial (Internet banking)

- You venture into Cyber Space when you
  - Use an ATM
  - Do Internet banking
  - Make a credit card payment

- **Of course you expect Cyber Space to be secure**
  - One of the most lucrative areas for cyber criminals
  - Electronic Identity theft
  - In SA about 4 billion rand py
Medical devices and systems using Cyber Space

- Medical devices (Heart pacemaker, Diabetes pump, etc)
  - your doctor can most probably monitor the pace maker and even adjust certain parameters if needed via Cyber Space
  - diabetes pump managed via cyber space
- Pacemakers can be hacked and can cause death
- Doctors have disabled the wireless capabilities of Former US Vice President Dick Cheney's pacemaker's to prevent cyber paced attacks on him.
  - Tele-operations
  - Tele-medicine
  - Tele-surgery
Water supply

We all assume we will have a constant and reliable water supply at our homes, offices, hospitals, schools, malls etc. In many cases, water grids are managed and monitored via the Internet, which is Cyber Space.
Travel

• Most modern airliners and ships are using operating and navigation software which are dependent on networks and very often Cyber Space.

• Well documented reports of the cyber-based systems of aircraft, ships, vehicles etc been hacked into
Personal privacy

All of us have massive amounts of private, confidential and sensitive data stored on databases spread over Cyber Space. These include:

- medical databases,
- Government databases,
- financial databases,
- retailer databases,
- social networks and
- many more.

Such databases are mostly accessible via the Internet, and to keep such databases, and our data, secure, we need a secure Cyber Space.

‘Personal privacy ... in the 21st century both depend on protecting a set of systems that didn’t even exist until late in the 20th — the electronic web of information-sharing known as cyberspace.’
Personal Risks

- Identity Theft
- Cyber stalking
- Cyber bullying
- Financial loss
The Internet of Things

The modern development is to make more and more every day devices accessible and controllable via Cyber Space.

A growing number of ‘things’ are given Internet addresses and are managed and monitored via the Internet, and therefore Cyber Space.

Such ‘things’ include refrigerators, thermostats, cars, smoke detectors, watches, glasses, and just about every other appliance you can think of.

They are connected to Cyber Space to provide remote access or to monitor and collected data.
Having looked at all these dependencies on Cyber Space, what is the general feeling about the security of Cyber Space?

Can we really secure Cyber Space?

Let’s look at two recent reports
Verizon 2014 annual cybersecurity report:

'The bad guys are winning - It's not just your imagination. It's getting uglier out there in cybersecurity land.'
‘The number of (cyber) threats is growing exponentially. In 1994, a new threat was discovered each hour. In 2006, a threat was discovered each minute. By 2012, this had grown to a threat per second. By 2014, this number had leaped to over three per second.’
‘South Africa has the third-highest prevalence of cybercrime in the world after Russia and China, with between 80% and 84% of residents having fallen victim to some form of cybercrime.’

http://www.wbsjournal.co.za/articles/combating-cybercrime-919.html
• It is not possible to **totally secure Cyber Space**

• However, all stakeholders must work together to make Cyber Space **as secure as possible**

• **Who are the stakeholders?**
  
  • Government – primary stakeholder
  • Private industry
  • NGOs
  • Civil societies
  • Man in the street
What is Government doing from their side?

- Very little at present
- No SA National Cyber Security Policy
- No Public-Private Partnerships to
  - Create a national culture of Cyber Security
  - Create Cyber Security capacity
  - Protect Critical Information Infrastructures
  - Protect SMMEs
Republic of South Africa

Review Report

E-commerce, Cybercrime and Cybersecurity – Status, Gaps and the Road Ahead

Final Version
26 November 2012
• small companies contribute on average 55% to SA’s overall GDP and 61% to employment.

• 66% of such small companies have online websites and

• 70% of these small companies acknowledge that business without a website would not be possible

• small businesses are reported to be the largest growth area for cyber attacks

• 31% of all attacks targeted small businesses, as SMMEs are less prepared to handle cyberrisks

• ‘SMMEs typically do not have the financial and human capacity to deal with cyber threats. … SMMEs specific cybersecurity programs can be the key to address (national) cybersecurity risks’.

Department of Communications of the SA Government, ‘E-commerce, Cybercrime and Cybersecurity – Status, Gaps and the Road Ahead’
• Biggest problem in securing Cyber Space in SA

  • No cooperation between Government and other stakeholders
  • No ‘face’ for Cyber Security in Government
  • No ‘face’ for Cyber Security amongst other stakeholders

• Some light at the end of the tunnel!!

• Minister of State Security

• Budget Speech and follow-up workshop
  • Invitation (will act as ‘face’)

• Creating an initial ‘face’ in industry

• Meet shortly
Conclusion

• We are all part of Cyber Space

• We are all under attack by cyber criminals

• We are all stakeholders who must apply pressure where ever we can to get a more secure Cyber Space for SA

• Let’s work together to secure it!
Thanks

basievs@uj.ac.za