NATIONAL SCIENCE AND TECHNOLOGY FORUM

ACEIE, CSP & NSTF workshop on digital wellness in SA

Jansie Niehaus

Exec Director, NSTF

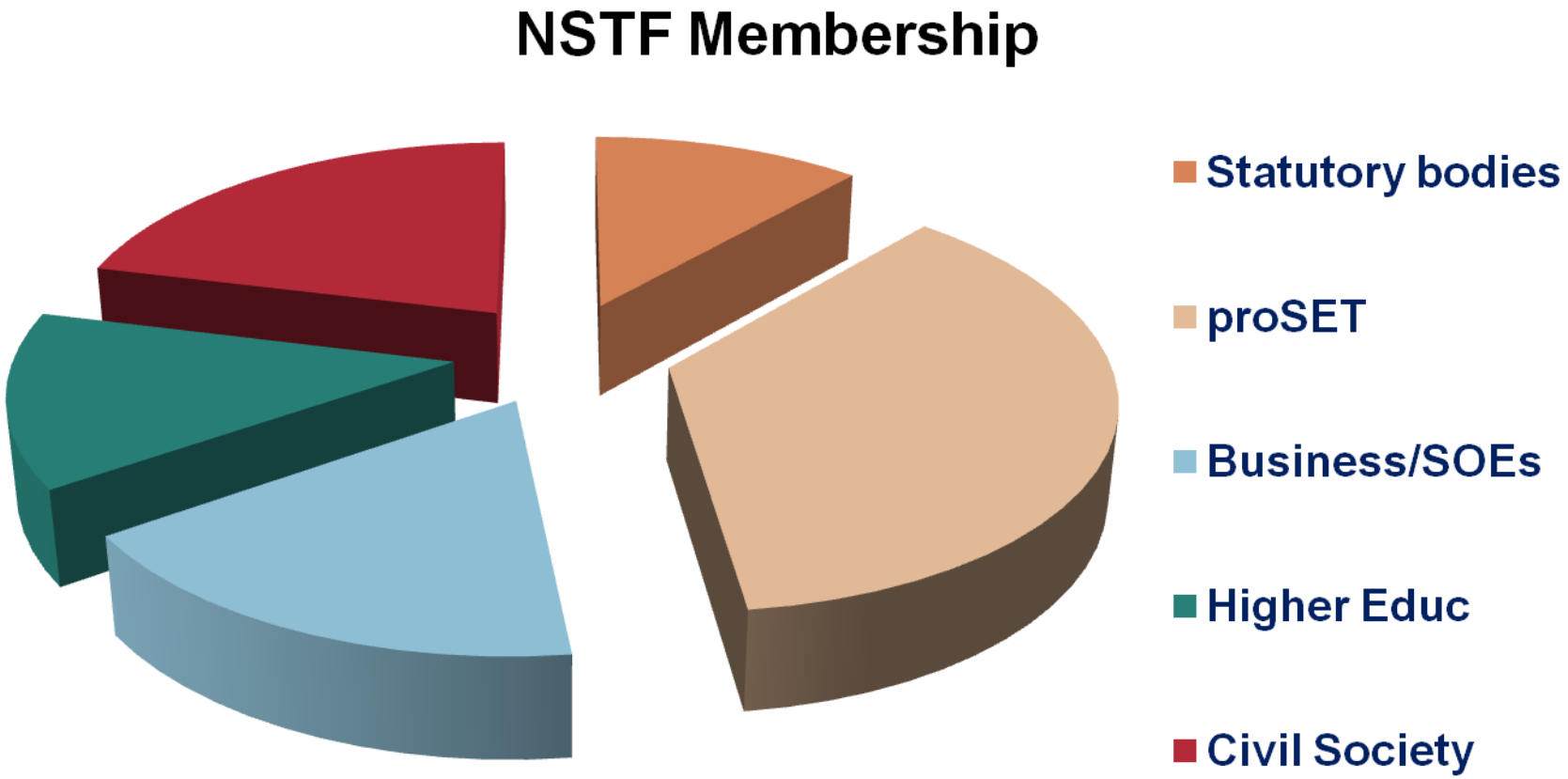
21 Aug 2015

S.E.T. for economic growth

Introduction to the NSTF

- National Science and Technology Forum, since 1995
- Non profit stakeholder body
- Representing all sectors related to science & technology
- > 110 member organisations

NSTF = Stakeholder Forum



Report on 15 May 2015
NSTF Discussion Forum

“ICT Security and Privacy Issues”

- *Information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without the talking about the other. ~Bill Gates*
- Urgent need for awareness and action.

Aims of the discussion, 15 May:

1. informing the science and technology community of the safe use of Information and Communication Technologies (ICTs),
2. to identify gaps in the applicable legislation, regulations and institutional measures

15 May Programme

- **Prof Basie von Solms**, Director: Centre for Cyber Security, Academy for Computer Science and Software Engineering (University of Johannesburg) - 'Why is a secure Cyber Space essential in SA?'
- **Mr Steve Jump,** Head of Information Security Governance, Telkom – 'Keeping your information safe, wherever you are'
- **Brig Piet Pieterse – '**The work of the SAPS Cyber Crime Unit'

15 May Programme, cont.

- **Dr Khaled Qasameh**, Department of Public, Constitutional & International Law, UNISA – 'Effectiveness of the legal framework governing cyber security at nuclear facilities'
- **Benson Lechaba and Erin Klazar,** ACEIE – 'Privacy vs surveillance: An investigation into the information ethical challenges faced by e-government services'
- **Keitumetsi Tsotetsi,** blogger on geekulcha
- **Andrew Ford,** Information Security Architect, Networks Unlimited

Questions:

- How well do the providers of various platforms look after the privacy and security of their users' data?
- As non-ICT experts, what can we as professionals do in this regard?
- What legislation is relevant for protecting the individual's privacy and research data owned by individuals, companies or institutions?
- What research is being done to address such issues?

Questions & answers:

- How well do the providers of various platforms look after the privacy and security of their users' data? It varies, but there is no accountability & transparency. Nothing is 100% secure.
- As non-ICT experts, what can we as professionals do in this regard? Look after our own data security, be aware & informed, hold our institutions accountable
- What legislation is relevant for protecting the individual's privacy and research data owned by individuals, companies or institutions? POPI Act, IP legislation
- What research is being done to address such issues? UJ, UP, NMMU, Unisa

Prof Basie Von Solms, Director: Centre for Cyber Security, UJ

- **Information can be accessed anywhere including unauthorised access and data interception.** identity and password theft, leading to masquerading and potential financial loss.
- **It is impossible to secure cyber space. we don't know the boundaries or the rate at which computers are connected.** Massive amounts of private, confidential and sensitive data are stored on databases accessible through the internet. We don't know where it is stored and how secure it is.

Towards solutions…

- Who is certifying security and why are companies not being held responsible for inadequate security?
- Tamarkin says that we need to know the scope of the problem before tailoring a response. Impartial statistics.
- To help collect stats on cybercrime: go to Centre for Cyber Security (UJ), http://adam.uj.ac.za/csi/ Click “report cybercrime” (since June 2015)

Recommendations

Stakeholder collaboration

- To make cyberspace as secure as possible, all stakeholders need to work together. Stakeholders include government, private industry, NPOs, civil society and the general public.

SA needs

- a national cyber security policy,
- a government entity directly responsible for cyber security,
- adequate legislation,
- cyber security standards, &
- public-private partnerships for creating a national culture of cyber security & developing capacity.

Ability to report to the police

- We need a process for reporting cybercrime affecting the general public. While there is specialised capacity through the SAPS Electronic Crime Unit (ECU), it has limited resources.
- Brigadier Pieterse, Section Head: ECU, Directorate for Priority Crime Investigation (Hawks), Commercial Crime, says that part of the solution is to train all detectives in cybercrime thus increasing capacity. This will assist with identity theft which is not receiving the attention needed from law enforcement.

Awareness and training at a user level

- A national programme of cyber security awareness is needed. Von Solms says that there should be a particular focus on schools. Learning materials have been developed but need government buy-in to progress further.
- South African Cyber Security Academic Alliance www.cyberaware.org.za - academic research groups from *NMMU, UJ and UNISA*. “vital life-skill”

Make cybercrime reporting mandatory

- **Transparency and governance:** We have no idea of the scope of the problem.
- Companies are reluctant to report because of the impact on the brand, the loss of competitive edge and financial loss.
- E.g. banks cover the losses from scams without publicising or declaring the size of the problem to anyone.

Move some of the responsibility *from* the user

- There is a drive to make ISPs (internet service providers), suppliers and other ICT entities more responsible for cyber security, such as downloading patches and making the default security setting as high as possible.
- E.g. Automatic installation and updating of software, and Ad block should be a default