

Trust (s)

TRUST in the INFORMATION SOCIETY
León, Spain 10th & 11th of February 2010

eu 2010.es



International Cooperation in Trust and Security

Republic of *South Africa*

Dr Barend J E Taute, CSIR
Prof Jan Eloff, SAP

THE BEST-RUN BUSINESSES RUN SAP

SAP

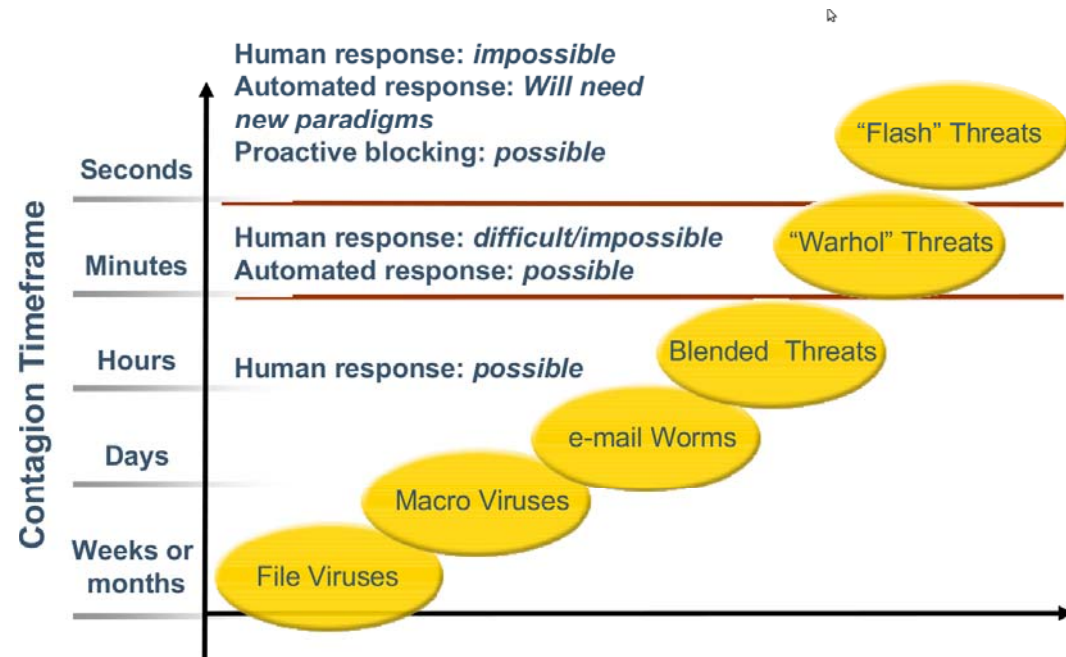
CSIR

our future through science

Challenging **Global** Issues of Trust, Security and Dependability

- Technological
 - It is getting more complicated again - usable security needed
- Societal
 - “need for speed” and latest vs knowing the consequences
 - Awareness and access to good advice required
- Governance
 - Reaching general compliance to known solutions
 - Legislation, regulation, forensics slower than new technology and mischievous use
- Programmes
 - Do we wait for a crisis?

(from presentation by Julia H. Allen, Networked Systems Survivability/CERT, Software Engineering Institute, Carnegie Mellon University)



Local Headlines

A Call to Cyber Security Action: Think Globally and Act Locally

by Dan Lohmann, Lohmann on GovSpace



32 people have been arrested in South Africa over a £12.8m spyware fraud

Cyber-crooks sting South Africa for £13m

Fraud went undetected for three years

Robert Jaques, vnunet.com, 11 Jun 2008

A cyber-crime syndicate is believed to have defrauded the South African government of more than £12.8m in a series of spyware frauds.

The crimes were revealed by the South African Minister for Finance and Economic Development, and have resulted in 32 arrests in connection with more than 80 separate fraud counts.

- News
- Opinion
- Business
- Sport
- Lifestyle
- Multimedia
- Special Reports
- MyNews24
- News
- South Africa
- World
- Africa
- Entertainment
- Science & Technology

Hackers steal R5.5m from dept

2009-10-13 08:38

Buks Viljoen

Pretoria - Suspected cyber hackers have stolen a total of R5.5m from the bank account of the education department in Mpumalanga, presumably with inside help.

The thieves even went as far as to first transfer the money from the department's bank account

FIFA World Cup

ESPN Soccernet | Sections | Live Scores | Home | How to qualify | Fixtures/Results | Europe | S.America | Concacaf | A

NET CLOSING ON FAKE WEBSITES

Cyberpolice crack down on World Cup ticket fraud

By Soccermet staff

September 25, 2009

Scotland Yard's e-Crime Unit has helped to save thousands of football fans from buying bogus tickets for the 2010 World Cup finals following a successful crack down on bogus internet sites.

FIFA called in the London-based unit to tackle the

of next year's

a police

ed down and

d the world.

the 32

lead to the

e wave could

approaches and

at illegal ticket

Click here to

bet365
Bet Now

FIFA Wo

- Zidane to fi
- Pokerman
- Winning co
- Klinsmann
- Zidane: Ma

One FIFA's special World Cup ticket ATMs.

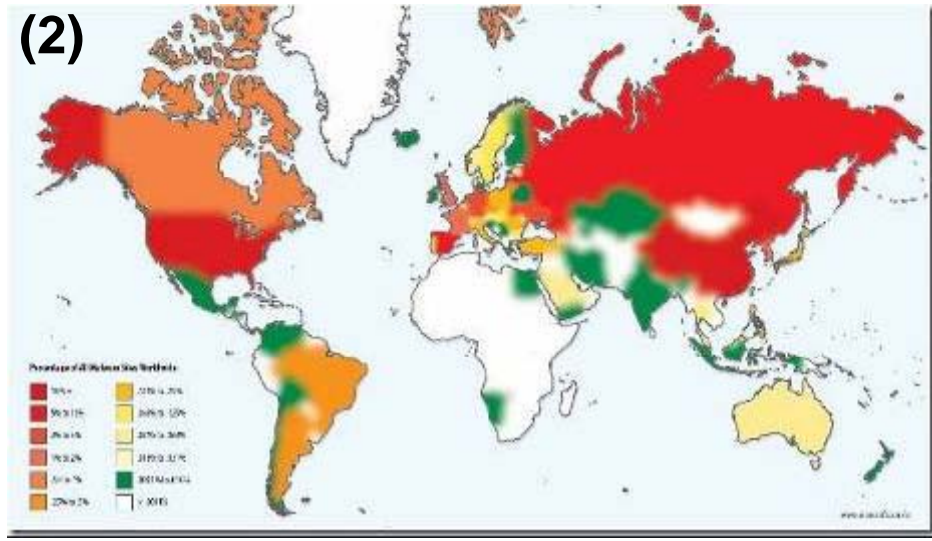
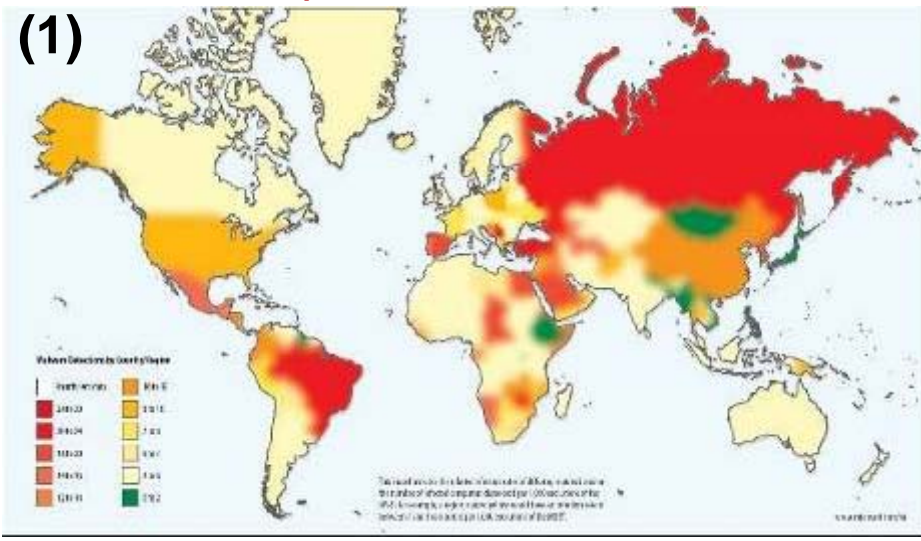
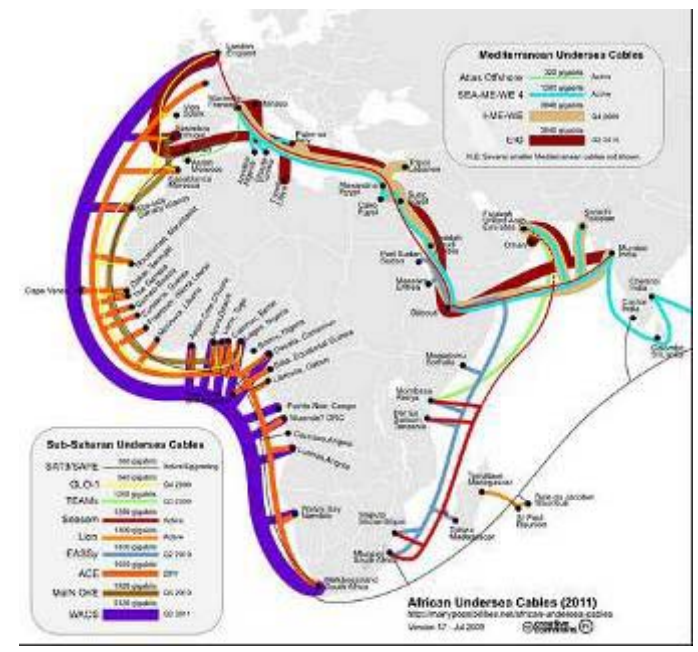
Symantec – 2010 FIFA World Cup to Increase Level of Cyber Crime in South Africa

According to an online security news, as the 2010 FIFA World Cup is approaching and extremely poor online security infrastructure, the incidents of cyber crime in South Africa are bound to rise because it is

malcke said: "Our

The advent of broadband to Africa by 2010/11

- ~100 million PCs in Africa,
 - poor security and old OS's
 - From standalone PC / dial-up to broadband online speed
 - IntelliBriefs 4/10/2009
- (1) Current average malware infection
- (2) very low source of malware hosting
- Could become a pandemic and launch pad for *international* cyber attacks
 - MS Security Intelligence Report Vol 6, Apr 09



South African features

- Internet penetration < 10% of population
 - High % of big business, medium % of local government and SMEs
- Privacy important but not a big political issue
 - Electronic Communications and Transactions (ECT) Act, Regulation of Interception of Communications Act (RICA) Act etc,
 - **but can we implement, monitor, investigate...?**
- Trust a concern but does not stop online transactions
 - Internet banking, e-Tax, e-NATIS, ...
 - ID theft, Phishing challenge for banks
 - Credit card fraud a regional challenge
- Bridging the digital divide
 - Technology “leapfrogging” opportunities
 - Drive to connect rural areas – opportunity, risk and threat
 - **Naivety, lack of awareness, culture of trust, lack skills to clean up**
 - High penetration of mobile phones, for some the 1st and only connection
 - **Need *usable security* given limited resources / skills / devices**
- National cyber security
 - Government agencies – policy and mandate overlaps, skills needed
 - Innovation track record, slow-down, no national R&D agenda
 - “turn-key solutions” vs local innovation and customisation
 - Critical infrastructure protection emerging understanding

Key *issues* from a 2009 Industry Survey by BMI TechKnowledge re *Information Security*

- Specialised + day-to-day **skills** shortage.
- Low security **literacy**
- Digital **forensics** and prosecution skills
- **Staff** misuse of ICT – convergence of physical & data security
- **Sophistication** of cyber crimes
- **Mobile** phone / removable device security risks
- Control over **digital identities**
- **Data protection** and information leakage
- Lack of central threat **detection** and coordinated **response/CSIRT**
- Security **economics** – the ROI argument
- World class products but lacking delivery, support, **implementation**
- **Banks** are fairly confident but need standards, eg online banking
- **Build security into SW** vs patchwork of solutions
- **Proactive** information security technologies needed

The following gives some South African (SA)

perspectives/programmes/needs

in the light of the Recommendations of the RESEPTIS Report

THE BEST-RUN BUSINESSES RUN SAP

SAP

CSIR

our future through science

1. Research agenda for Trustworthy ICT

Recommendation 1

The EC should stimulate interdisciplinary research, technology development and deployment that addresses the trust and security needs in the Information Society

Priority Areas

1. Security in (heterogeneous) networked, service & computing environments
 - SA – cloud, open source roll-out, eGovernment strategy, lack Research Agenda
 - SA - Digital forensics research – static, live, wireless
 - SA – SANREN high-speed research network ↔ GIANT in EU, Certif Auth in RSA
 - Controlled sharing of IP rights in networked org's
2. Trust, Privacy and Identity management frameworks
 - SA – PKI legislation, implementation framework needed, crypto build skills
 - SA – Home Affairs National ID System; RFID in paper, vehicle licence
3. Eng principles & architectures - trust, privacy, transparency & accountability
 - SA – tools to verify privacy assurances – support eGov, mCommerce
4. Data and policy governance and related socio-economic aspects
 - SA – King III report on corporate governance

2. The interplay of technology, policy, law and socio-economics

Recommendation 2

The EC should support concrete initiatives that bring together technology, policy, legal and social-economic actors for the development of a trustworthy Information Society

- Technology development without strong regard for the societal context, economically, socially and legally, will lead to the loss of trust
 - SA
 - National Cyber Security Policy in process – Dept of Comm's, ITU response
 - Strategic independence needed in key areas (source code, response, ...)
 - Alignment of legislation and mandates needed
 - Exploitation of **opportunities** enabled by trustworthy ICT

3. A common European framework for Identity Management

Recommendation 3

A common EU framework for identity and authentication management should be developed that ensures compliance with the legal framework on personal data protection

- Design that guarantees the principles of privacy, minimal data disclosure, proportionality and legal framework
 - SA – HANIS project, PKI framework
 - SA – Constitution, Electronic Communications & Transactions Act,
 - Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) Act – demands IDENTITY COMPLIANCE – contracts + prepaid customers
 - Protection of Personal Information Bill
 - Information Security and Information Access Control processes will be required once enacted
- Instruments for forensic analysis
 - SA – pockets of excellence, skills shortage

THE BEST-RUN BUSINESSES RUN SAP



4. Further development of EU legal framework for data protection and privacy

Recommendation 4

The EU data protection and privacy legal frameworks should be further developed, as part of an overall consistent ecosystem of law and technology that includes all other relevant frameworks, instruments and policies.

- The relationship with other policy frameworks - consumer law, liability for products and services that collect and process data
 - SA – King III report on Corporate Governance – responsibility to protect privacy
 - SA – credible way to verify privacy assurance in public and private sectors?

5. Large scale innovation projects

Recommendation 5

Large-scale actions should be developed towards building a trustworthy Information Society which make use of Europe's strengths in communication, research, legal structures and societal values

- Techno-legal ecosystem for trust, security and privacy, amenable to global cooperation, boost growth, basis for international cooperation.
 - **European data processing in the Cloud;**
 - SA – e-Government skeptical despite benefits, need for considered use
 - **Services platform with EU legal framework and governance infrastructure;**
 - SA – eGovernment vision, needs coordinated implementation
 - **Next-generation social networks, interoperability and privacy;**
 - SA – eHealth provision to rural areas / data privacy
 - **EU-wide, legally accepted electronic documents**
 - SA – Medicines Regulatory Authority implementation of EDMS
 - SA – eHealth, archiving, RFID in documents, ...

6. International cooperation

Recommendation 6

The EC should address the global dimension and foster engagement in international discussions, as a matter of urgency, to promote the development of open standards and federated frameworks for cooperation in developing the global Information Society.

- International understanding, cooperation and interoperability, joint international measures and standards on governance, anti-crime measures, identity management, security and other relevant topics.
 - SA
 - EU Cybercrime Convention – signed, not ratified – implementation needed
 - CSIRT cooperation – ENISA, Finland, ... Progress but need statutory mandate.
 - ISO standards committees – active participation
 - ESASTAP: participation in EU FP7 calls – Security + ICT Themes
 - Participation in COST Actions – access to scientific thinking

Conclusions

- SA can benefit from EU
 - Learn from cyber security policies / strategies / research agendas / legislation / organisational structures
 - Collaborative projects and S&T networks (FP7, COST, etc) – computer crime, forensics, critical infrastructure protection, privacy..
 - Skills transfer, human capital development, organisational structures
- SA could aid and complement EU
 - Technology adaptation for use in developing countries
 - Unique combination of world class financial infrastructure and third world / rural economy
 - Use cases for mobile solutions in rural areas
 - mCommerce, mGovernment
 - Collaborative crime prevention, incident response
 - Collaborative next generation / future internet opportunities

THE BEST-RUN BUSINESSES RUN SAP

