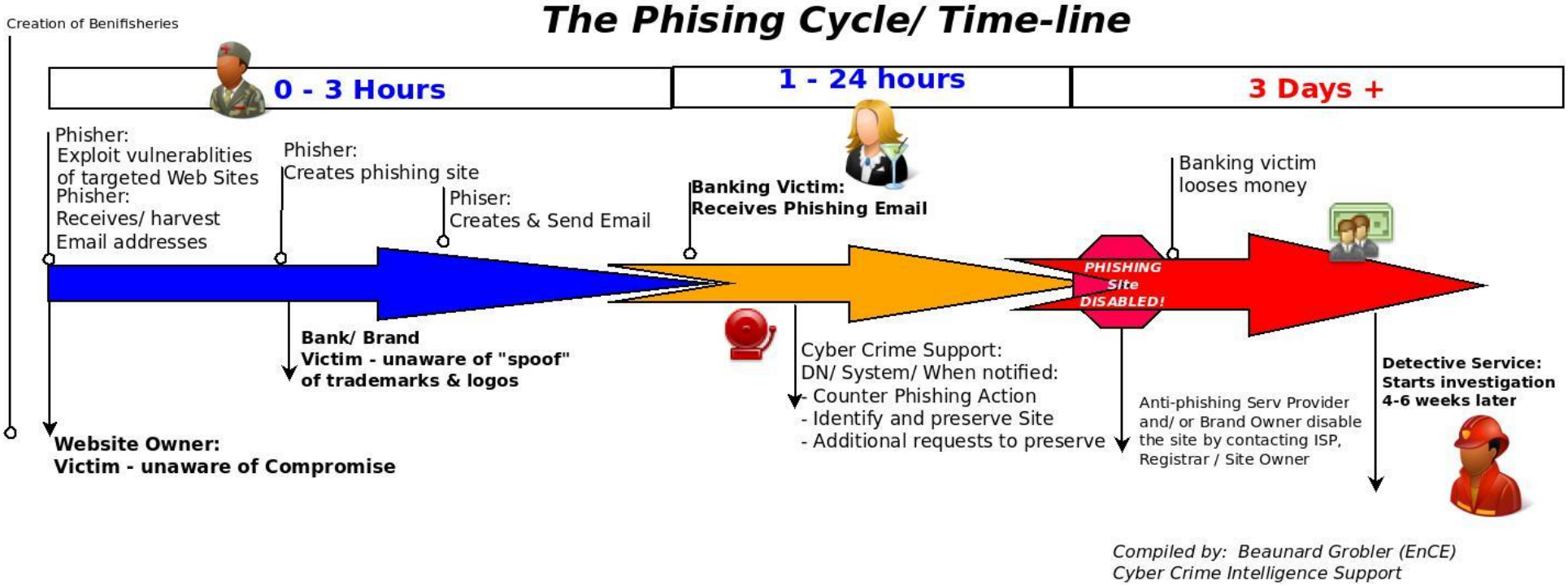
Data exchange architecture used in a financial application in South Africa

Dr Barend Taute
CSIR Meraka Institute
South Africa

6 July 2011

CSIR

our future through science



- Relative ease + availability of phishing software
- SIM swap, “man in the middle” and social engineering
- Cash-out: beneficiary account, ATM, cellphone airtime, MPESA ….
- Phisher, exploited website, phishing website, email harvesting, banking victim could all be in different countries

The Challenge

- South Africa 4 % of world's phishing volume
  - Currently 4th in the world (down from 18%, 3rd) after USA, UK, India
  - Still new victims, increase in local phishers
  - National Computer Security Incident Response Team (CSIRT) planned
- Phishing → malware and spyware (creative, targeted, less visible)
- Combating Phishing
  - Banks: Close down (via service provider)
  - Police: Investigation + forensic evidence
    - Mutual legal assistance required
    - Privacy and "no local victim / complainant"
    - Trust as basis for international intelligence sharing
    - Quick International Cyber Legal Assistance is needed
- Cyber Security Awareness needed (users at all levels)
  - Developing world: Low comms → broadband. Vulnerable + potential host
  - Creative ways to internalise the message (games, videos, …)
- Network attack prediction and visualization – research project
  - Network telescopes etc → attack taxonomy → alerts and data sharing

Financial Sector

- 6 banks with internet banking, including one-time-password to cellphone
- Served by the SA Banking Risk Information Centre
- Already gather and share crime related information
  - Considering privacy, reputational risk, not legally binding to report
- Public-private partnerships to combat crime
- Banking CSIRT in planning phase
- A sector level data sharing architecture:
  - Focus on crime prevention rather than investigation
  - Privacy limitations
  - Sharing “suspicious information” could be less contentious but strict client confidentiality is still essential.
  - Common “negative database”
  - Client consent to share for crime prevention is needed
  - Sector → local ISPs → international banks foreseen

Thank you

Contact details: **Barend Taute**
Telephone +27 12 841 4063
Email btaute@csir.co.za
Web www.csir.co.za

our future through science