Towards a Cyber Secure Society

4th Biennial Conference

Presented by WA Labuschagne

9 October 2012

our future through science

Critical Infrastructure

- Describe assets that are essential for the functioning of a society and economy (Wikipedia)

Critical Infrastructure

- Examples
  - Energy
  - Transportation Systems
  - Nuclear Reactors, Materials and Waste
  - Banking and Finance
  - Postal and Shipping
  - Communications
  - Information Technology

Is It Possible?

- Sewage and water treatment system
  - Australia in April 2000 (Vitek Boden)
  - Took control of the SCADA system (Wireless connection)
  - Released of raw sewage

Is It Possible?

- 2002
  - Venezuela Port
  - Country's main port (Disabled)
- 2003
  - Ohio Davis-Besse Nuclear Plant
  - Plant safety monitoring system (Shut down)
- 2005
  - Daimler Chrysler
  - 13 U.S manufacturing plants (Shut down)

Is It Possible?

- Estonia (April 2007)
  - First cyberwar
  - Three-week wave of distributed denial-of-service attacks
  - Crippled country's information technology infra-structure

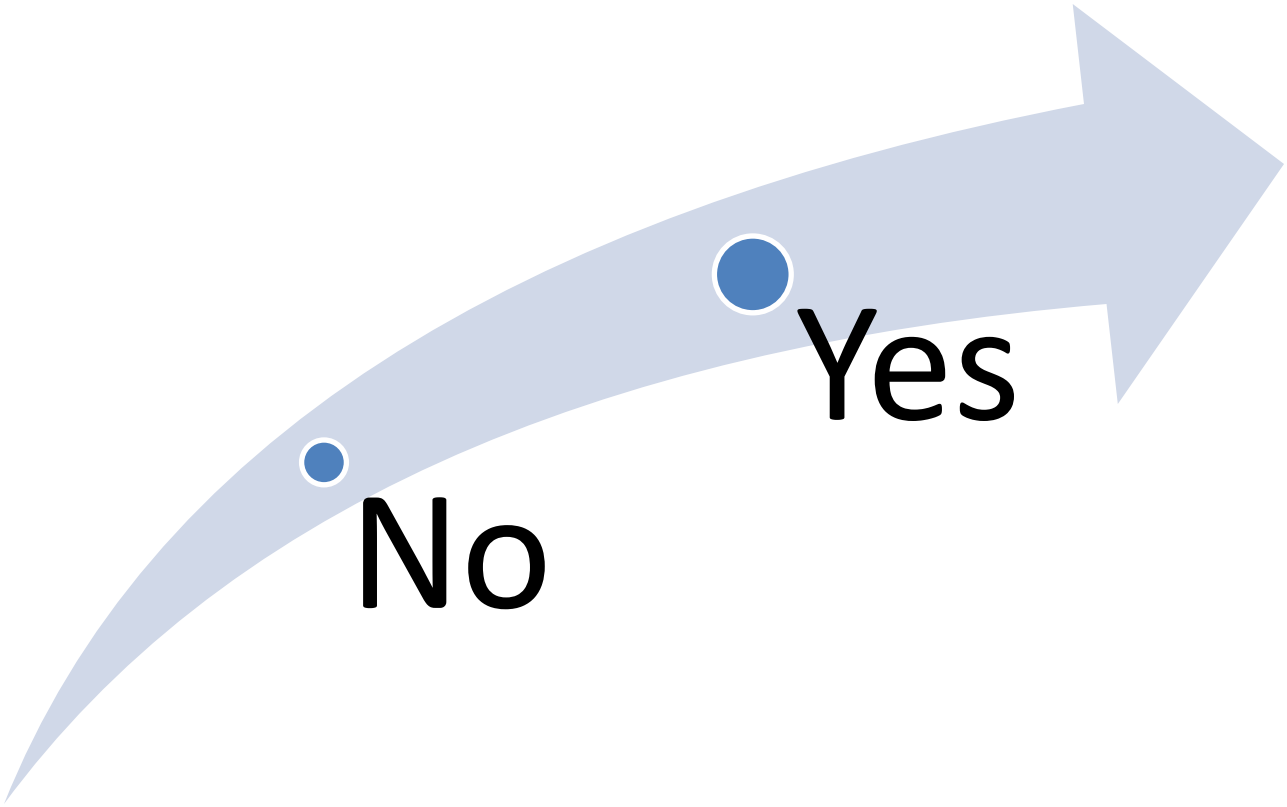
Is It Possible?

- Stuxnet
  - Discovered in July 2010
  - Target was Iranian nuclear facility
  - Cause refinery's centrifuge to malfunction
  - Air-gapped from outside networks (difficult to penetrate)

Is It Possible?

- Anonomous
  - Hacktivism Group
  - Targets
    - Mastercard & Sony
      - Web site down
      - Hacked servers

Is It Possible?



What is possible

- South African Postbank (January 2012)
  - Loss of estimated $6.7 million
  - Remote access
  - Transfer money to created accounts
  - Fraud detection system (Failed)
  - Crime was discovered only after employees returned to work (After the holiday)

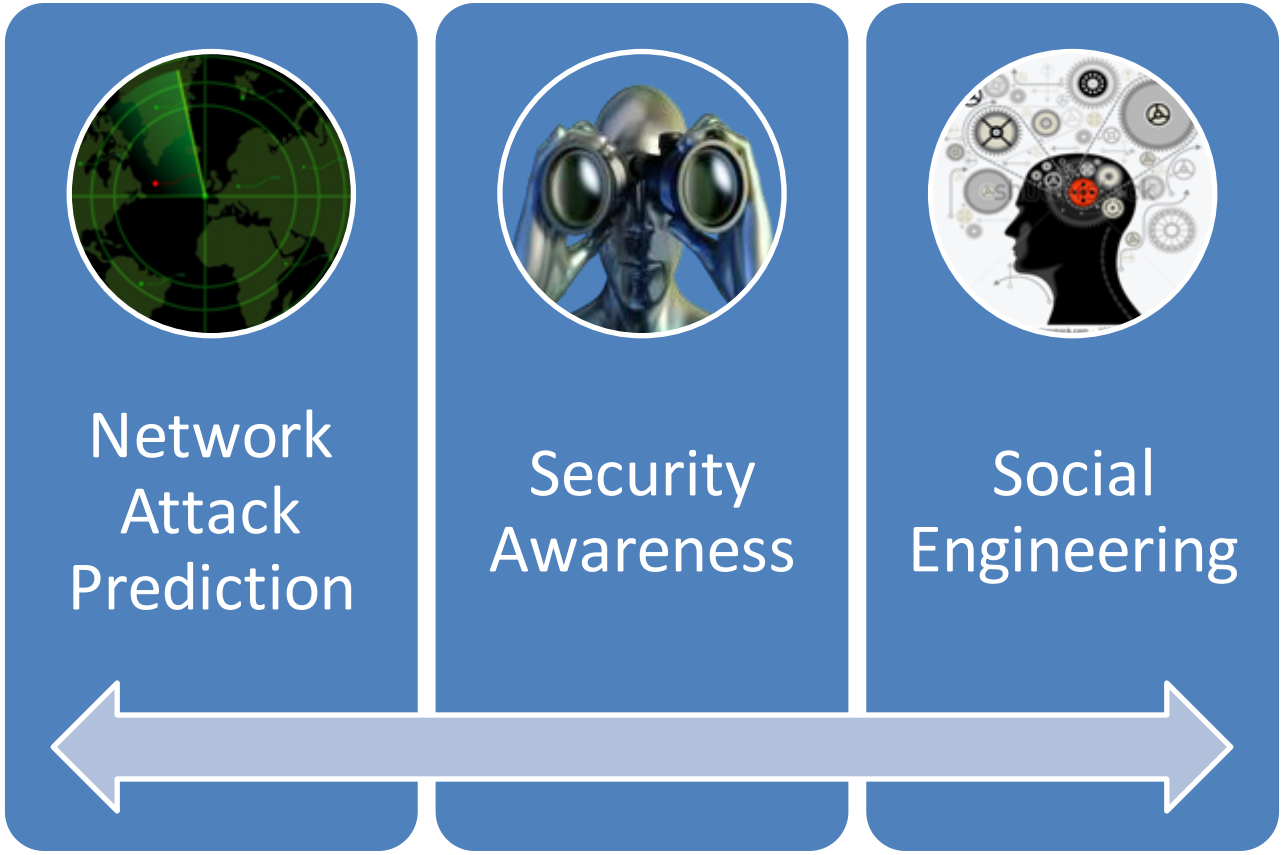
What is possible

- The power of Social Media
  - Arab Spring (18 December 2010)
  - Revolutionary wave of demonstrations and protests
  - Rulers have been forced from power in Tunisia, Egypt, Libya, Yemen
  - Civil uprisings have erupted in Bahrain Syria

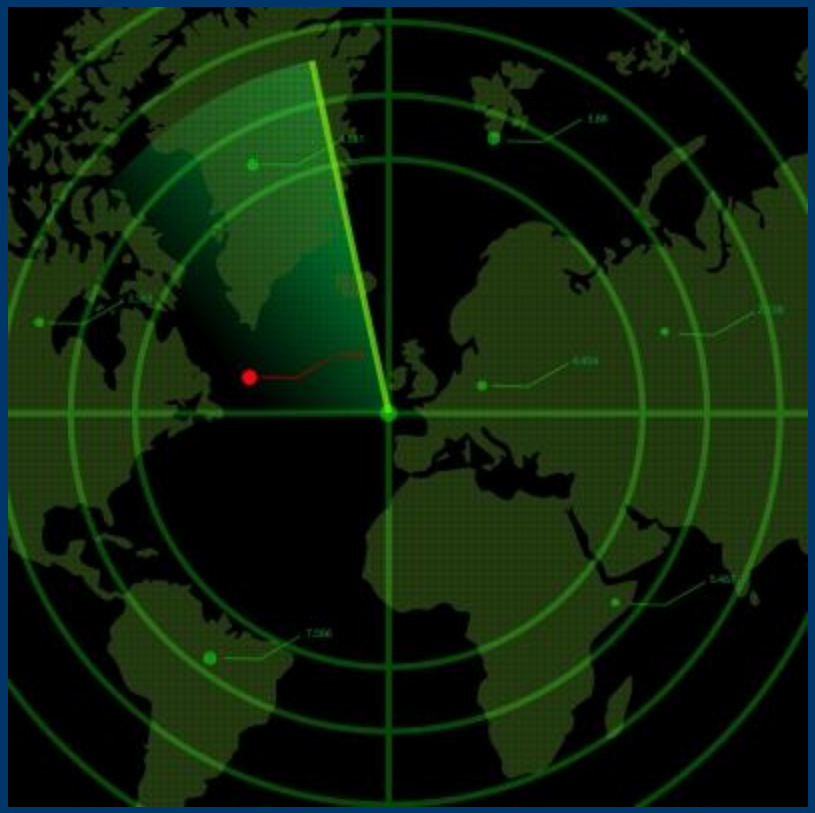
What is possible

Java™

Cyber Defence Areas



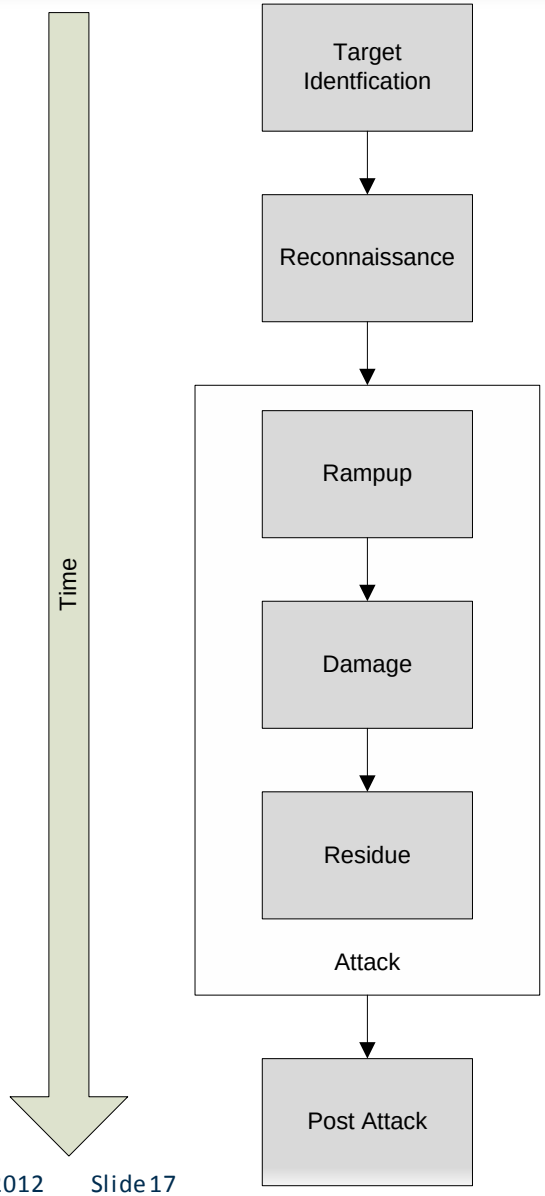
Network Attack Prediction



Network Attack Prediction

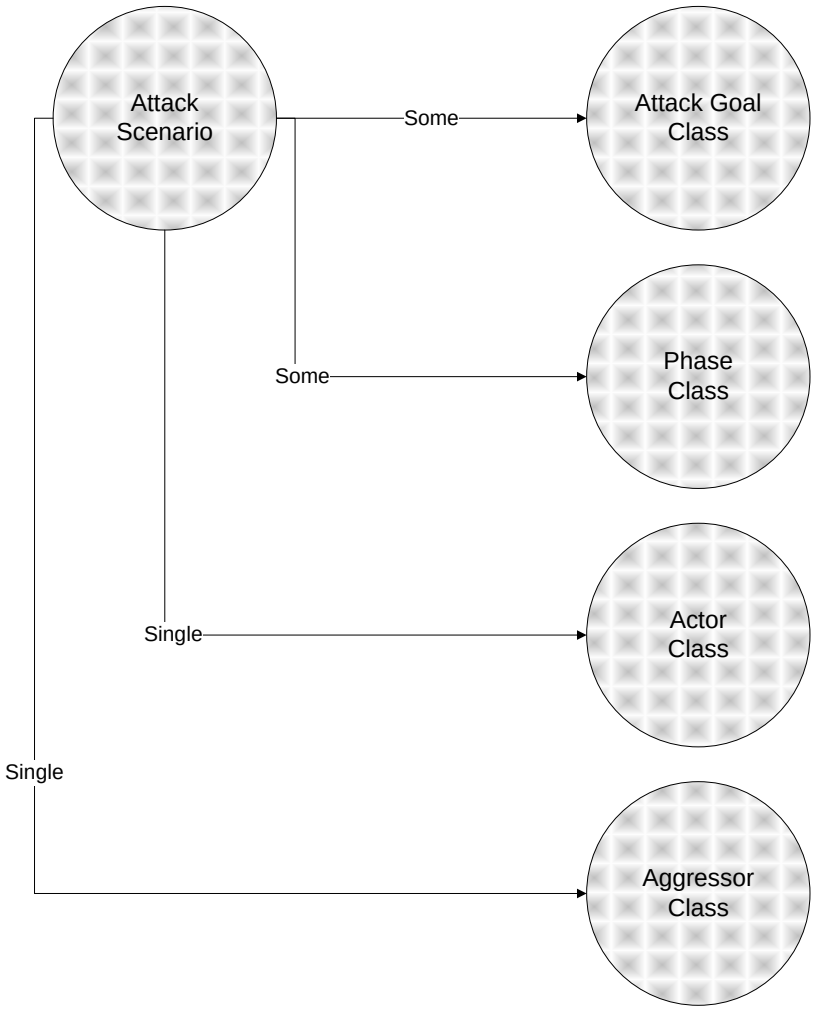
- The Internet is the battle space for cyber warfare
- Internet viable environment for warfare without declaring war:
  - The cost of launching attacks are very low compared to traditional warfare
  - The interconnectivity makes it possible to effectively hide the origin of any attack
- Early warning system

Temporal Attack Model



Attack Scenarios

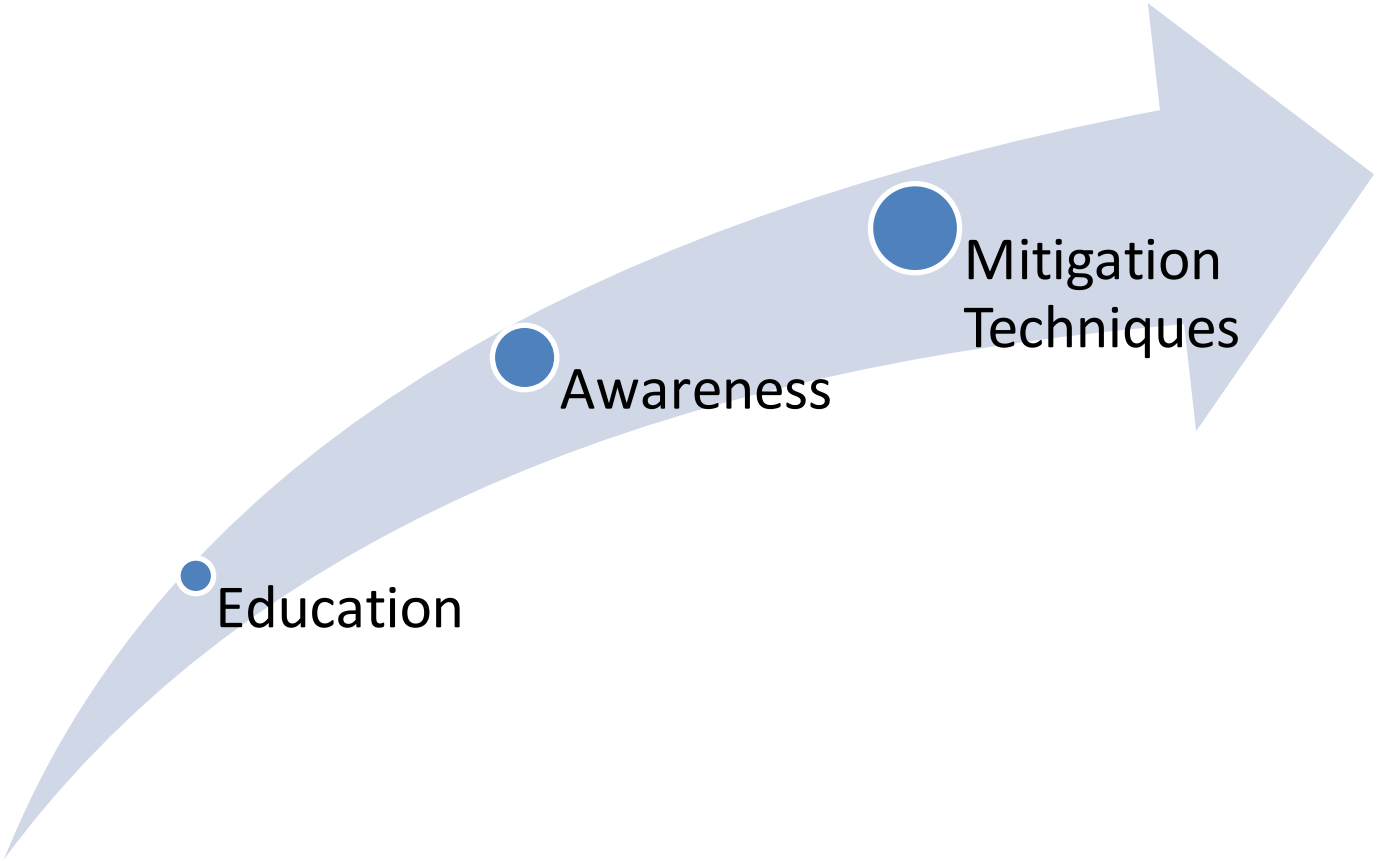
- Denial of Service
- Industrial Espionage
- Web Deface
- Spear Phishing
- Password Harvesting
- Snooping for Secrets
- Financial Theft
- Amassing Computer Resources
- Industrial Sabotage
- Cyber Warfare



Security Awareness

Motivation for the project

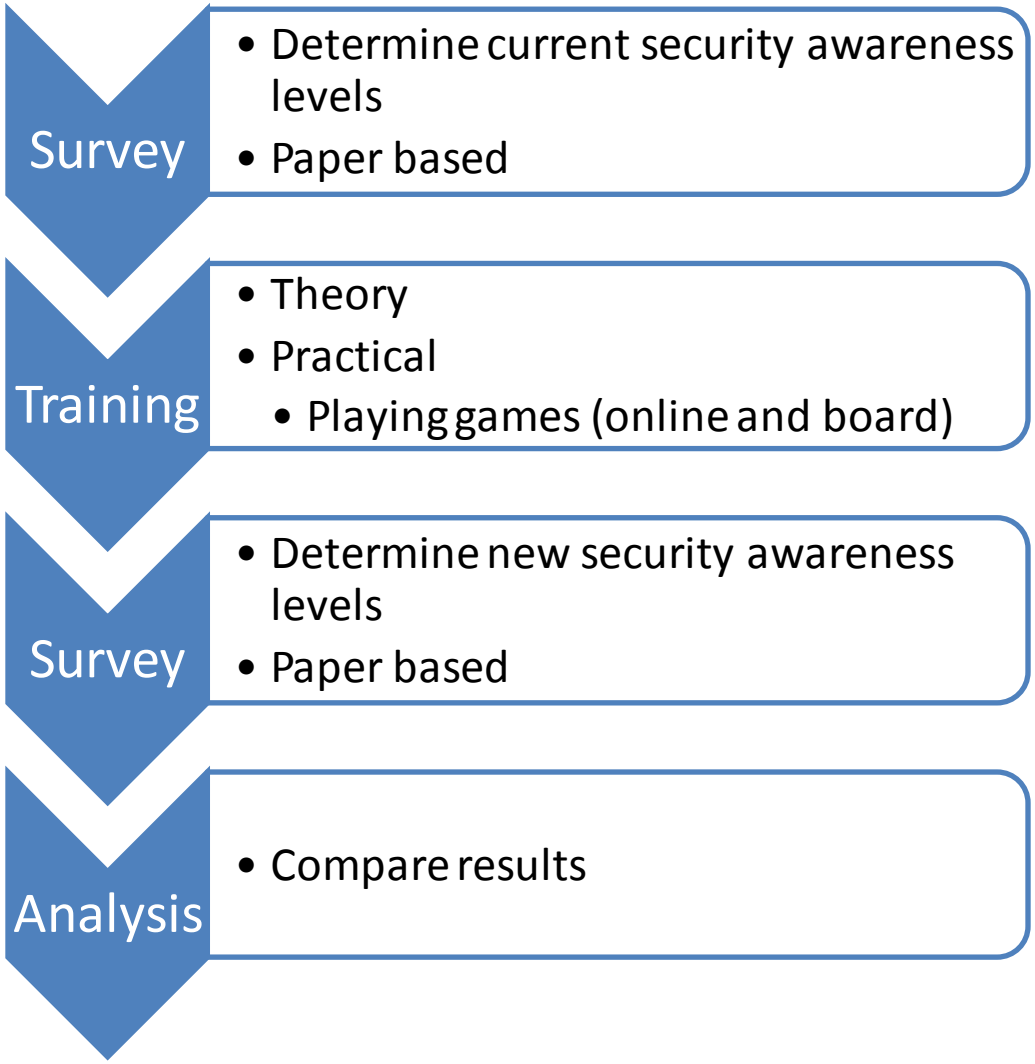
Cyber Security Awareness Training



Target Audience

- Primary schools
- Secondary schools
- Further Education Training colleges
- University (technical and non-technical)
- Community centres
- Support staff
- Educators/Teachers

Security Awareness



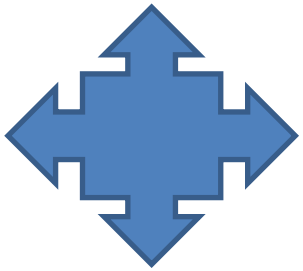
Compare Results

Trained so far

- About 45 student volunteers
- More than 550 community members!

Social Engineering

The Good Side of Social Networking Sites

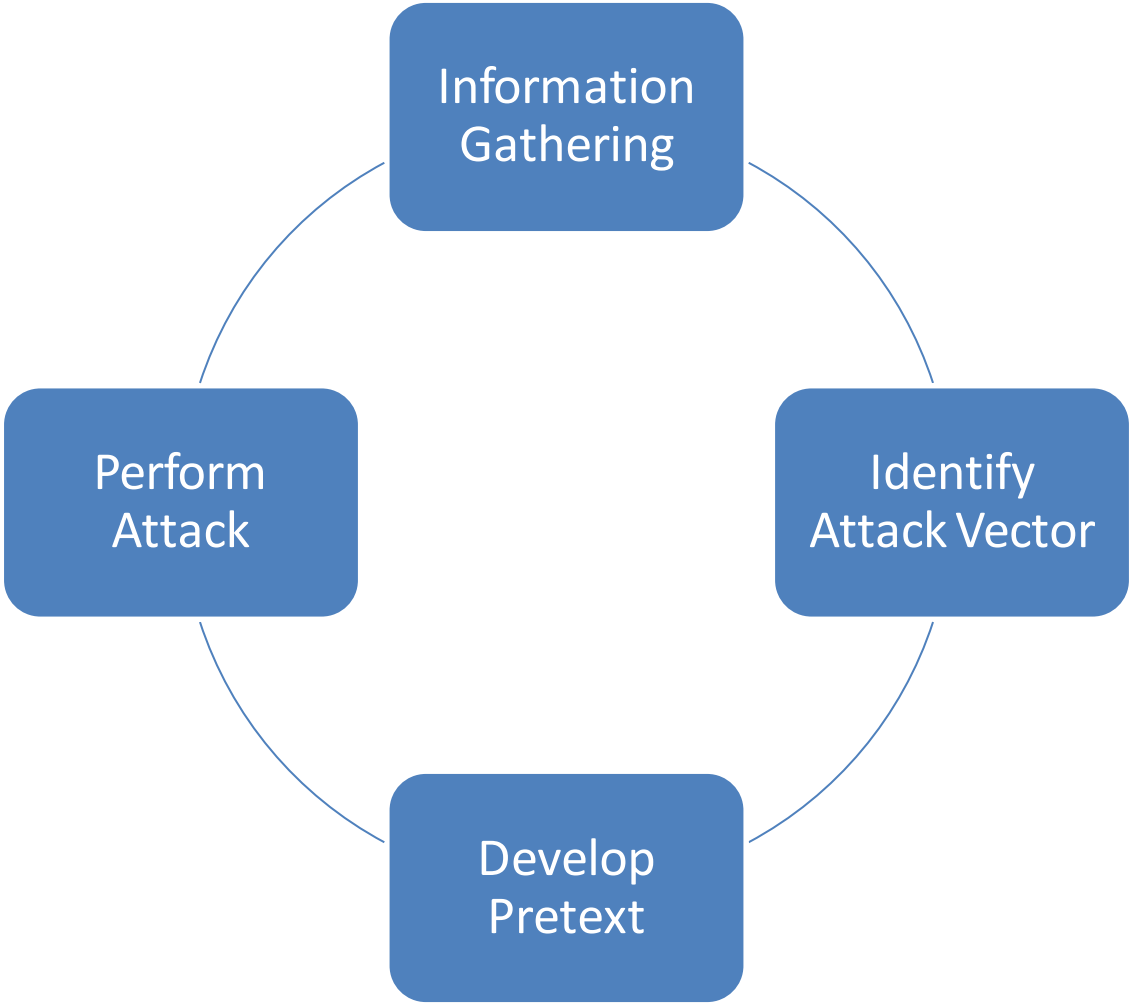


The Dark Side

Social Engineering

- The art and science of **getting people to comply to your wishes**
- **Getting needed information** (for example, a password) from a person rather than breaking into a system
- Art of manipulating people **into performing actions or divulging confidential information**

Social Engineering Cycle

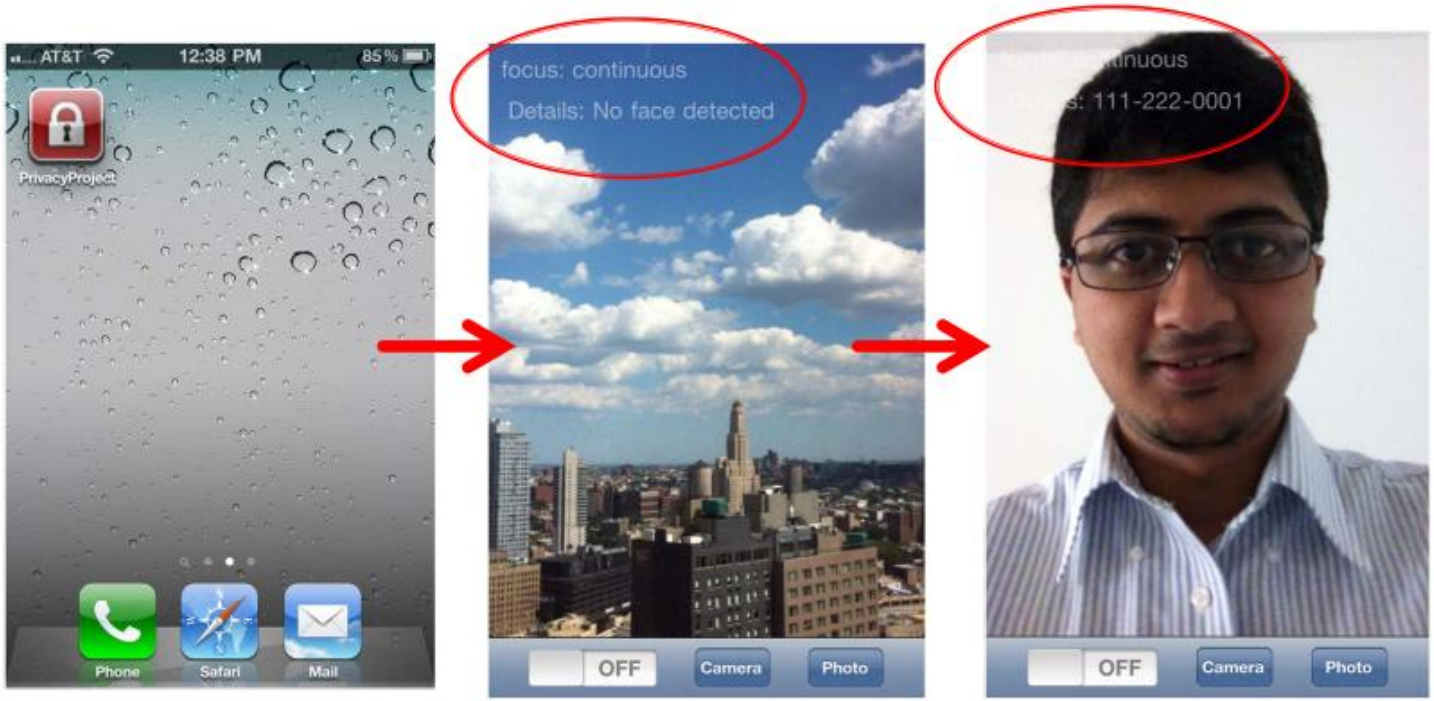


Digital Profiling

- Use of digital footprint to profile user
- James W. Pennebaker
  - Linguistic Inquiry and Word Count (LIWC)
  - Text analysis software program
  - Identify social relationships, emotions and thinking styles from textual data
- Robert Layton
  - Authorship Attribution for Twitter

Digital Profiling

- Alessandro Acquisti (Blackhat 2011, USA)



Experiment (Published at HCC 2012, Amsterdam)

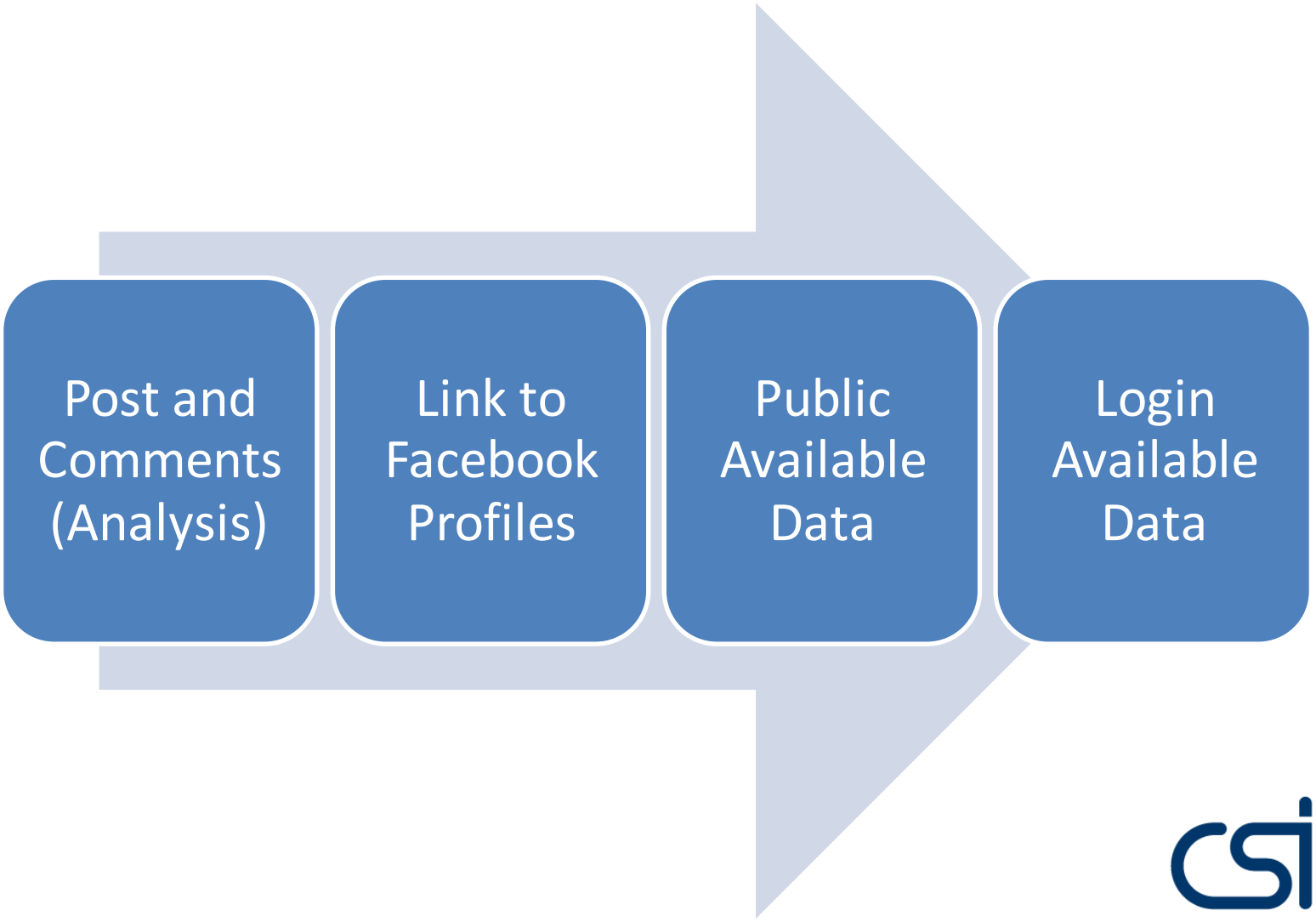
Article

- Theme
- Objective

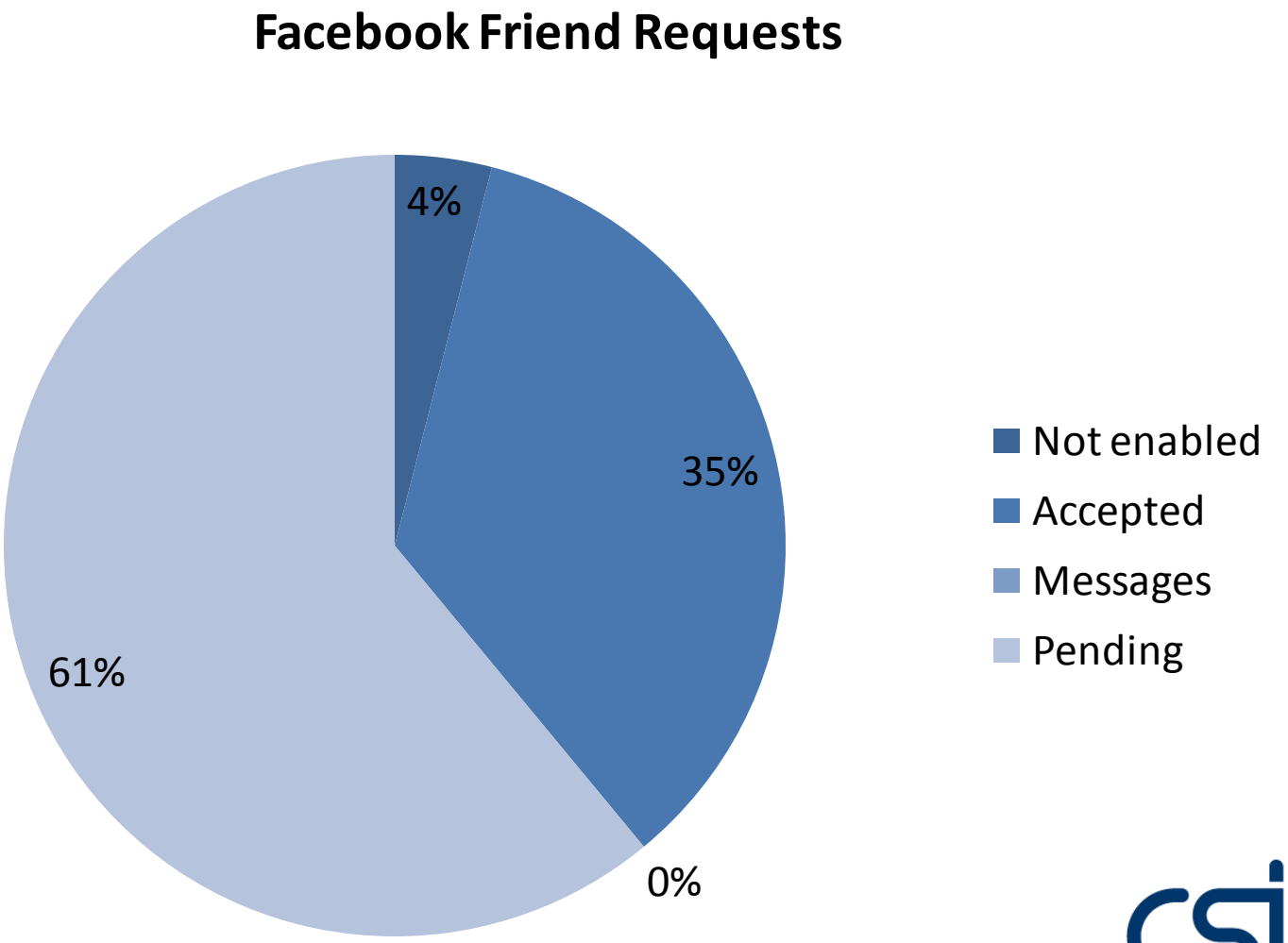
Posts

- View
- Subjective

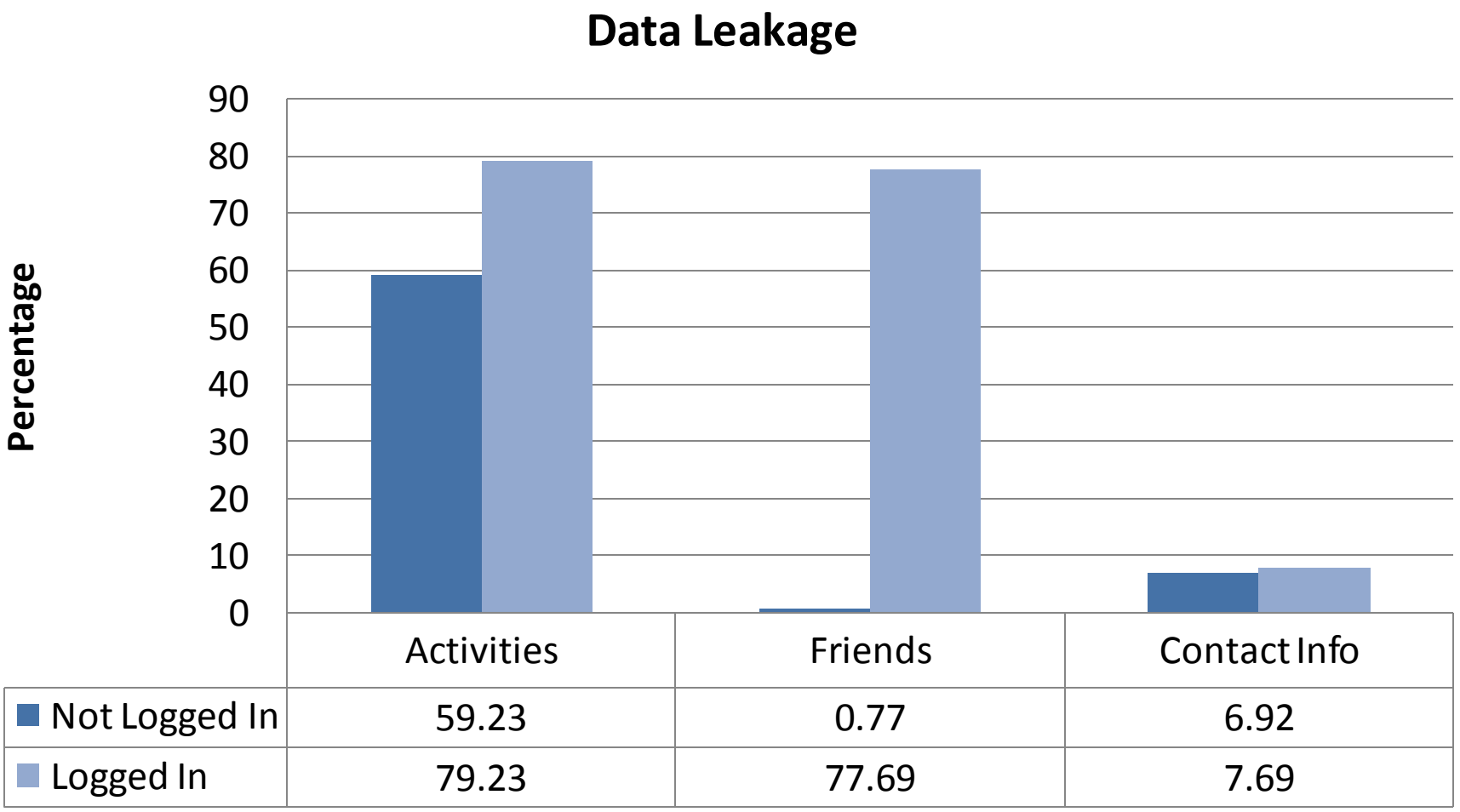
Experiment



Findings (1)

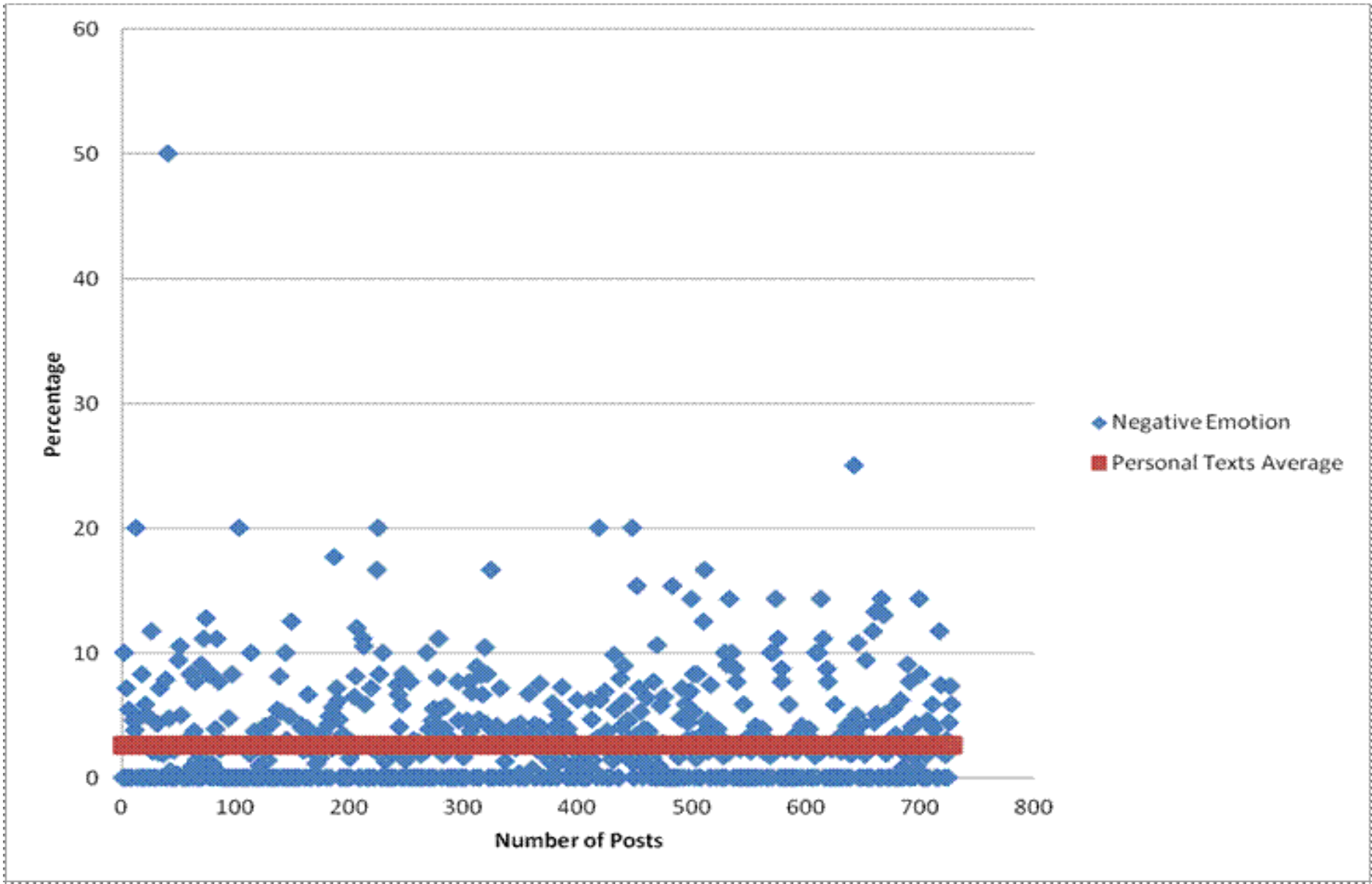


Findings (2)

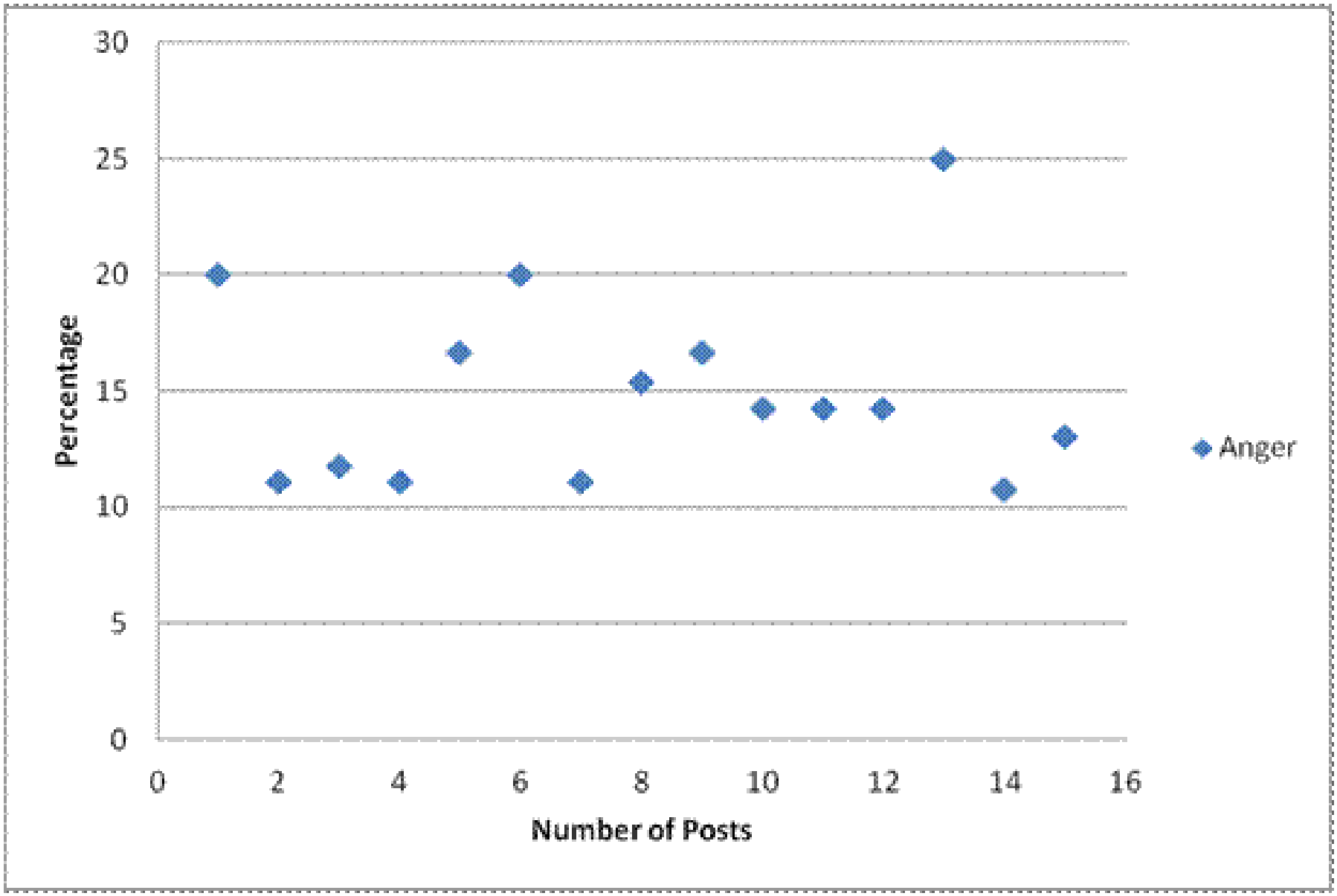


	Activities	Friends	Contact Info
Not Logged In	59.23	0.77	6.92
Logged In	79.23	77.69	7.69

Analysis of Posts



Anger Emotions above 10%



Discussion

- Use of target profile information:
  - Topic that evokes emotion
  - Create custom targeted attack (Social Engineering Toolkit)
  - Create fake profile (Friend List)
  - Deliver via Facebook email
- Security Awareness
  - Users do not apply privacy settings correctly
  - Friendship request are not questioned
  - Platforms are implicitly trusted
- Digital footprint dangers

For Your Interest

National Systems

- Financial Systems
- Medical Systems
- Biographical Information
- Regulation of Interception of Communication Act (South Africa)
- Trapwire (USA) - Facial recognition technology

Google

- Interests (Search Terms)
- Contact Lists
- Messages
- Facial recognition technology

Facebook

- Social Graphs
- Friends
- Interest
- Activities
- Facial recognition technology

Conclusions

- Dependence on information technology increases
- Cyber attacks are becoming complex
- Attack vector is growing
  - Digital footprint dangers
- Understanding of threat is critical
- Security Awareness
  - Provide people with techniques to mitigate threats

Thank you

our future through science