Information Security

Overview of Paradigms and Scenarios

John Ngubiri

Overview

- Introduce Government Information Security
- Information Security - Paradigm shift impact
- Aspects Information Security Management
- Information Security Problems and Threats
- Practices related to Information Security and Privacy
- Necessity for Information Security plan, policy and training
- Information Security and Disaster Management

Background

- Information Security
  - Safe guarding information from unauthorized access/threats (digital or not)
  - Fuelled by advancement in technology
  - Complicated by information virtualisation
  - Connectivity is assured, problem is rights
  - Portability is easy, cheap and seamless
  - Change of station is easy and cheap
  - Systems manipulatable
- Change of paradigm
  - Work habits: from physical to ubiquitous
  - Proliferation of personal into organisational security
  - BYOD - complexes
  - Connectivity, excessive outsourcing
  - IT naivity of some experts

Concerns

- Work life and social life are intertwined
- Social web applications defacto modes of official collaboration/communication
- Less regulation in the mix of work and social life
- Working from home or ubiquitous working is on the increase
- Access to the ever growing amounts of personal data on organizations and peoples profile
- Assurance on proper use of personal data by custodians

Information Security Management

- A process of achieving objectives using a given set of resources
- Managerial Roles
  - Informational role: Collecting, processing, and using information to achieve the objective
  - Interpersonal role: Interacting with superiors, subordinates, outside stakeholders, and other about the information
  - Decisional role: Selecting from alternative approaches and resolving conflicts, dilemmas, or challenges about the information
- Any role not well done can be problematic
- The system can actually be ”threatened”

Threats

- Representation of possible danger
- Danger can affect the
  - confidentiality
  - Intergrity
  - Availability
  - Accountability

  of information
- Threate may be
  - Physical threats: fire, floods, terrorist, activities and random acts of violence
  - Electronic threats: hackers, vandals and viruses
- Dependant on your situation:
  - What business,
  - who you are,
  - how valuable information is,
  - how your information is stored,
  - who has (legitimate) access to it etc..

Handling threats

- Threats have to be handled otherwise you are insecure
- Can be exhaustive and frustrating with a thorough approach
- The Ground is not level
  - They are so many: Cost, time, money .... may be too much
  - Some never actualise for centuries
  - Attacker exploits only one, you defend all
  - Some are actually low impact threats
- Addresing needs to be more strategic
- Need calmness – avoid analysis paralysis

Threat Modeling

- Assemble the threat modeling team
- Decompose the Application
- Determine the Threats to the System
- Rank the threats in Decreasing Risks
- Chose the Response per Threat
- Chose mitigation Techniques
- Chose mitigation Technologies

Vulnerabilities

- Organisational weaknesses exploitable by a threat
- Gateway for threat manifestation
- Docile untill when coupled with a threat
- inherent in complex systems and always present
- Could be:
  - incorrect configuration
  - poor physical security
  - poor hiring practices
  - etc
- Different types
  - Known: one that is easily detectable and probably security precautions are already taken
  - Unknown: one that is publicly available but unknown to the organization
  - Zero day: not publicly available and unknown to vendor

Attack Targets

- Communication Media
- Servers
- Software
  - OS
  - Application
  - Coockies
  - Web
  - Mail
- Hardware
- Middleware
- Users
- Peripherals

Digitisation and a Challenge

- With Digitisation, Security is more complex
  - Lots of data is created - creating leads
  - Connectivity is higher - the challenge can be access
  - Traffic is high - leaving traces
  - Technologies have improved - simulations/replays

The Social media problem

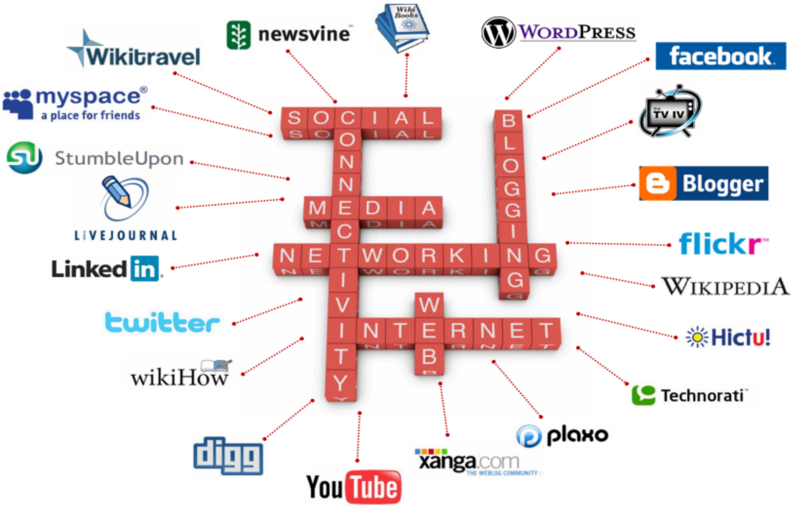

Figure: Where is social media

Basic Paradigm - SM

Connections/Linkages

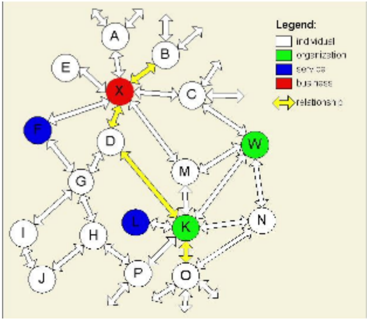

Figure: social connections

- Person linked to Person
- Person owns Business
- Business seeks Person
- Person works for Org
- A service
  - to organisations
  - to busisness
  - to individual
- Hybrids
- A mesh.....

Security??

Organisation!!

- Hosted on organization-owned or external infrastructure?
- Using organisational or provider technology?
- Open or closed to public?
- Who owns the data?
- How indemnified is the provider?
- What is the intrinsic benefit ?

Individual

- Level of Privacy
- Who owns your profile
- Who owns your data
- To whom is your data given

Some Considerations

General

1. Brand
2. Reputation
3. Productivity Loss
4. Intellectual property

Security

- Privacy
- Information leakage
- Hacking
- Breach of confidentiality
- Legal lapses

Some Partinent questions to address

- It is easy for ”hard copy” individuals to recognise each other. Failure to identify means no control on security. How is identification done in electronic scenarios?
- Hard copy data is easy to confine and secure, Electronic data can be stolen and remains. What are the general approaches in which data can be secured?
- What is the relationship between data security and Law?

The End