Lecture 4

Infocomm Security

Outline

- Information Classification
- Singapore Infocomm Security Masterplan
- Guest speaker: Mr. John Yong

  Director, Infocomm Security & Assurance

  IDA

Cyber-Threats

- Like other open economies, Singapore faces threat from all vectors
  - Epidemic
  - Terrorism
  - Threats to infocomm environment
- Challenges in protection of infocomm environment
  - Malware: worms, virus & trojan horses
  - Irresponsible hackers, cyber-criminals & cyber-terrorists
  - Ignorant users & system owners

Proactive Efforts in Cyber-Security

- Legislation Level
  - Examples
    - Computer Misuse Act in 1993
    - Electronic Transactions Act in 1998
- Policies & Guidelines Level
  - Examples
    - Infocomm Security Best Practices
    - Internet Banking Technology Risks Management Guidelines in 2003

Proactive Efforts in Cyber-Security

- Infrastructure Level
  - Examples
    - Public Key Infrastructure in 1996
    - SingCERT in 1997
    - Infocomm security awareness programme for people, private & public sectors
- Strategic Level
  - Examples
    - Infocomm Security Masterplan

Information Classification

Safeguarding Trust

- Failure will impact trust of citizen on Government & its systems
- Undertake upfront business impact assessment (BIA) & risk assessment
  - BIA identifies cost (financial & nonfinancial) of a set of business processes that are not functioning correctly
- Assess Confidentiality, Integrity, Availability (CIA) of information

Need for Classification (1/2)

- Classified information
  - Sensitive information to which access is restricted by law or regulation to particular groups of persons
- Formal security clearance is required to handle classified documents or access classified data
  - Clearance process requires a satisfactory background investigation.

Need for Classification (2/2)

- Typically several levels (classes) of sensitivity
  - Each has differing clearance requirements.
  - This hierarchical system of secrecy is used by virtually every national government
- Data classification
  - Act of assigning level of sensitivity to data

Info Classification in Government

- 4 major security classification of info
  - Top Secret (exceptional grave damage to national security)
  - Secret (serious damage to national security)
  - Confidential (damage to national security)
  - Restricted (undesirable for admin & security reasons)

  - Unclassified
    - Technically not a classification level, but is used for government documents that do not have a classification listed above
    - Such documents can sometimes be viewed by those without security clearance

Info Classification in Private Sector

- System classification for banks
  - 3 – 4 security levels
  - 3 classes of Internet financial services in MAS IBTRM

Clearance

- Depending on level of classification there are different rules controlling level of clearance needed to view such information, & how it must be stored, transmitted, & destroyed
- Access is restricted on a "need to know" basis
  - Simply possessing a clearance does not automatically authorize an individual to view all material classified at that level or below that level
  - The individual must present a legitimate "need to know" & proper level of clearance

Cyber Watch Centre

Background

- IM8D CWC policy has a wide coverage affecting all government web services & portals
- Intention was to provide capability
  - to constantly monitor cyber-threats to Government systems, networks & services
  - to detect & respond to cyber attacks in a timely manner
- Government systems, networks & services then were mostly on internally hosted infrastructure
  - Increasingly, more government systems, networks & services are outsourced or hosted externally, especially with advent of cloud computing services

Cyber Watch Centre (CWC)

- As of 2007, an IM8D policy on "Security Monitoring" requirements requires all government agencies with services running on systems deemed critical or high risk to use CWC services offered by eCop (through a bulk tender arrangement)

- CWC operates 24/7 to enable Government to better anticipate & respond to cyber attacks by continuous monitoring of situation

Critical or High Risk Systems

- For purpose of security monitoring, such systems are
  - Service-wide ICT Infrastructure & Systems
  - Government systems, networks & services that are directly accessible from Internet
  - Mission critical systems as defined by Government agencies that are connected to SGNET
  - ICT systems at Government agencies that facilitate investigation of security incidents

Exception

- Policy allows for specific exceptions, generally due to technical, operational or business constraints
- Agencies seek approval for exceptions through CWC Policy Working Group
  - Approving authority is National Infocomm Security Committee (NISC)

Infocomm Security Masterplan 2005

IS Masterplan 2005

- 3-year (FY2005-2007) strategic roadmap
- S$38 million seed funds to bolster cyber security & build capabilities
- Objectives
  - Defend Singapore's critical infrastructure from cyber attacks
  - Maintain a secure infocomm environment for government, businesses & individuals

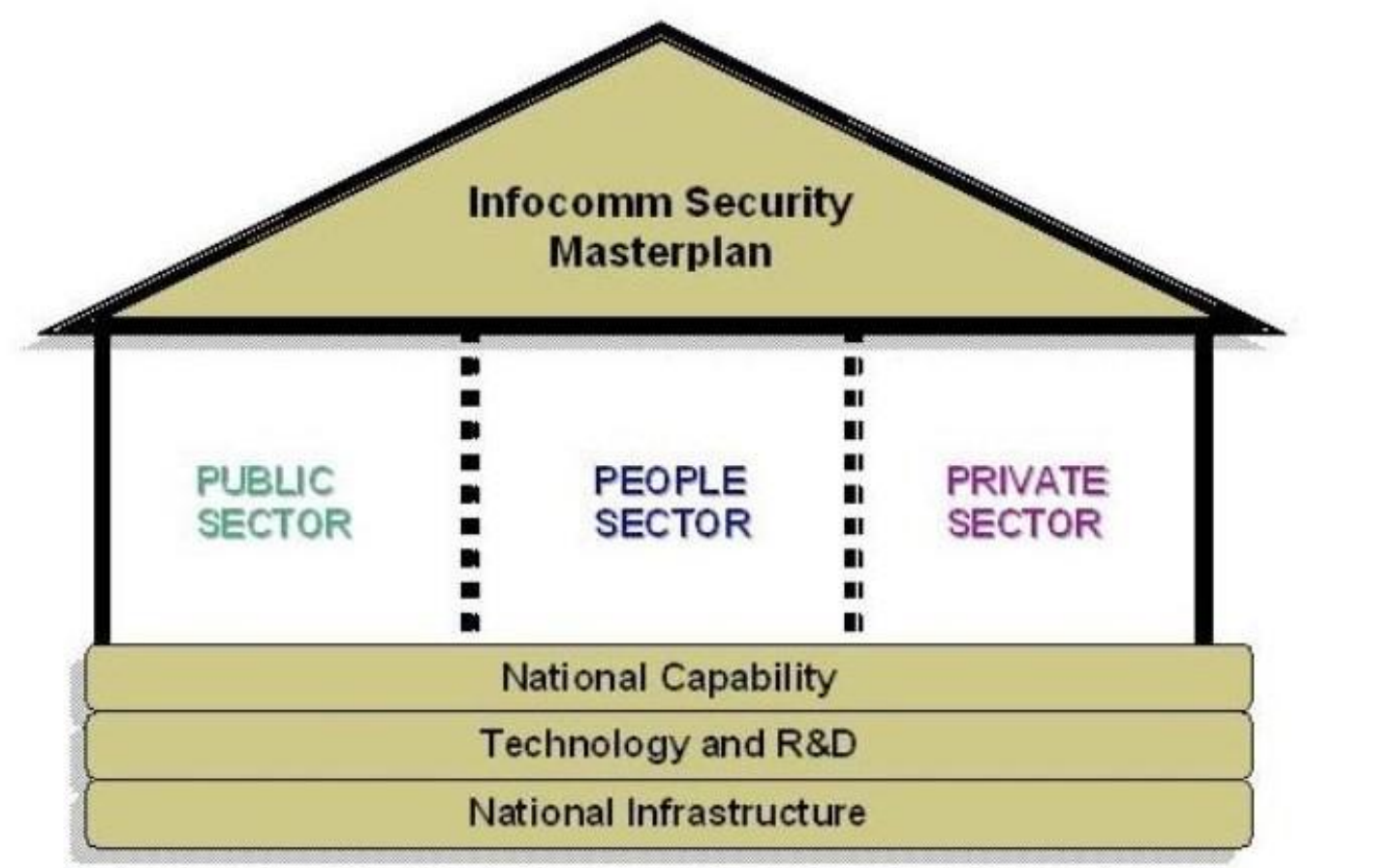
Development of Masterplan

- Multi-agency effort led by Infocomm Development Authority of Singapore (IDA)
- Driven by a high-level steering committee
- Inputs from businesses & government agencies

Strategies

- Six strategies
  - Securing the People Sector
  - Securing the Private Sector
  - Securing the Public Sector
  - Developing National Capabilities
  - Cultivating Technology & R&D
  - Securing National Infrastructure
- Projects will build upon existing initiatives

Strategies



Pictorial Representation of the Masterplan Framework

Key Outcomes

1. Enhanced situational awareness & contingency planning assurance
2. Information protection assurance & risk mitigation measures
3. Human & intellectual capital development

Enhanced Situational Awareness & Contingency Assurance

- Technical controls & processes are not enough
- Need to know what is going on in real-time
  - Ability to detect when an incident happened
  - React fast enough to prevent harm to our infrastructures & systems or to limit damage
  - Ability to restore system to its original state
- Example of initiatives
  - Cyber threat monitoring

Info Protection Assurance & Risk Mitigation Measures

- Risk Assessment
- Vulnerability analysis and reduction
- Technology assessment
- Example of initiatives
  - Vulnerability Assessment
  - Security Testing
  - Critical Infrastructure Protection
  - Security Health Scorecard

Human & Intellectual Capital Development

- Security Awareness
- Development of professional skills
- Promotion of research & development
- Example of initiatives
  - Awareness Outreach
  - Certification of Infocomm Security Practitioners

Public-Private Collaboration

- In implementing some Masterplan projects, there will be a need for government to engage private sector
- Businesses were consulted during planning of the Masterplan
- Expertise from solution providers needed in implementation

Conclusion

- Encourages change of mindset to treat cyber security with priority
- Infocomm environment & threats that it faces are ever changing
- Enhancing infocomm security, resilience & preparedness of the nation is a journey without end

Singapore Infocomm Security Masterplan 2010

Guest speaker

Mr. John Yong

Director, Infocomm Security & Assurance

IDA