هيئة الإتصالات وتقنية المعلومات
Communications and Information Technology Commission

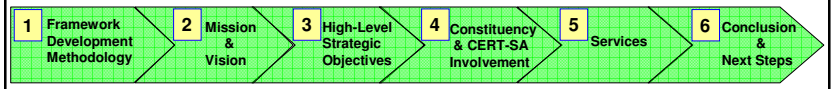
Round Table Discussion 1

CERT-SA
Vision, Mission & Services

Dr. Ahmad Sindi,
CITC Deputy Governor, Information Technology

Sunday, June 4, 2006

Agenda



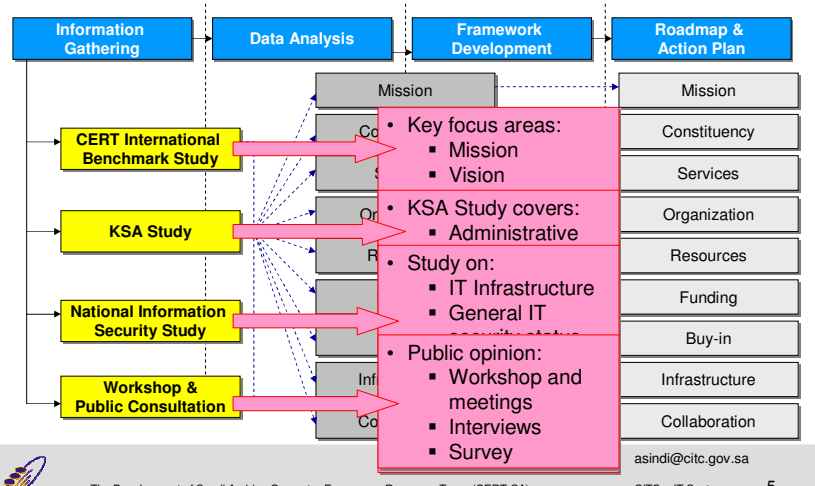
1. Framework Development Methodology
2. Mission & Vision
3. High-level Strategic Objectives
4. Constituency & CERT-SA Involvement
5. Services
6. Conclusion & Next Steps

Framework Development Methodology

Framework Development Methodology

- Proposed framework is driven by a methodology involving **four** components:
  1. CERT **International Benchmark** Study
  2. **KSA Study**
  3. National Information Security Study
  4. Public **consultation** process

Framework Development Methodology



International Benchmark Study

Benchmark of 10 CERT centers worldwide

Vision
&
Mission

Vision Statement

Our vision is

"To be the trusted authoritative reference for information security in the Kingdom of Saudi Arabia."

Mission Statement-1

Our mission is:

- *to boost the information security awareness level in the Kingdom of Saudi Arabia*
- *to coordinate national level efforts towards promoting best practices to help in preventing; deterring and dealing with information security attacks and incidents*
- *To suggest national information security policies, procedures and guidelines.*
- *to foster trust, cooperation and collaboration among our constituents and the general cyber community in the Kingdom*
- *to be the reference in information security for all agencies in the kingdom*

Mission Statement-2

Our mission is (cont.):

- *to provide advisory to constituents in the area of information security*
- *to build Saudi talent and human capacity in the field of information security in the Kingdom of Saudi Arabia*
- *to hold educational and awareness seminars, specialized training, and events about information security to the benefit of the general cyber community in the Kingdom*
- *Provide a trusted environment for e-transactions*
- *Coordinate with other CERTS regionally and Internationally*
- *to build and maintain CERT-SA with the most advanced technology and Equipment available in the field of information security*

High Level Strategic Objectives

High Level Strategic Objectives

Awareness: *disseminate accurate, timely and relevant information on IT security to all constituents and the public by 2007*

Development: *create, build and operate a world class CERT (possessing necessary talent, process and infrastructure) by 2010*

Service: *provide the necessary set of services and policy guidelines for that will help constituencies in performing their duties of prevention, detection, response & management of information security threats by 2007*

Response: *develop a coordinated national information security response by 2010*

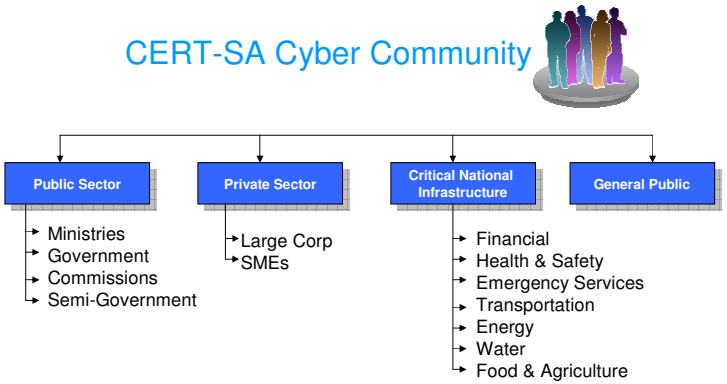
Constituency & CERT-SA Involvement

Constituency Options

- CERTs may have unbounded or bounded constituency:
  - Unbounded by providing the services to whoever request the services
  - Bounded to constraints such as national, geographical, political, organizational and others

Proposed Constituency

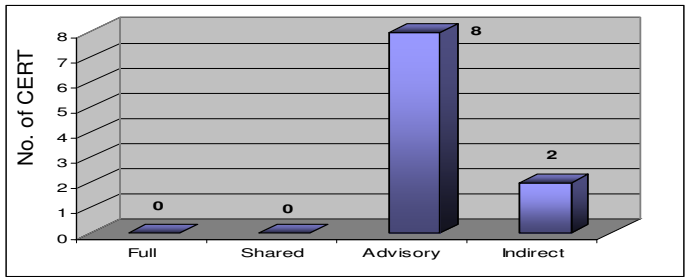
CERT-SA will have a **bounded** constituency



CERT-SA Involvement Options

Involvement	Relationship
Full	The Center has authority to take actions or decisions on behalf of its constituency
Shared	Direct support and share the decision making process (influential to the constituency)
Advisory	Acts as advocate/advisor – No implementation responsibility
Indirect	Able to exercise pressure for the constituents to take specific action

Proposed Involvement Options



Involvement Options

- Advisory Involvement – CERT-SA Cyber Community
- Indirect Involvement – ISP & DSP only

CERT-SA Services

Common CERT Services

Reactive Service
R1 - Alerts and Warning
R2 - Incident Handling
R3 - Vulnerability Handling
R4 - Artifacts Handling

Initiated by an event or request

Proactive Service
P1 - Announcement
P2 - Technology Watch
P3 – Selective Security Audit or Assessment
P4 - Configuration & Maintenance of Security Tool, applications & Infra
P5 - Development of Security Tools
P6 - Intrusion Detection Services
P7 - Security Related Information Dissemination

Provide assist. & information to help prepare, protect, & secure

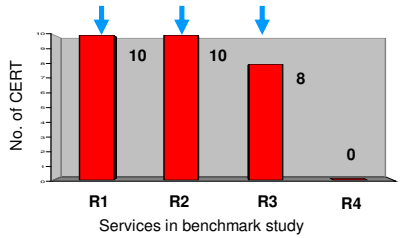
Security Quality Management Service
S1 - Risk Analysis
S2 - Business Continuity & DRP
S3 - Security Consulting
S4 - Awareness Building
S5 - Education/Training
S6 - Product Evaluation or Certification

Proactive but contribute indirectly to reducing the number of incidents.

Our criteria for service offering

- Reflect priority issues and observe lines of authority of various agencies
- Avoid potential pitfalls, learn from International Benchmark Study
- Start small and add more services once TRUST have been earned
- Do not offer too many services at one time, spreading resources too thin
- Do not compete with other information security provider, effective security through cooperation
- Wide adoption in the majority of CERTs
- Useful for most constituencies especially those with limited information security resources
- Service demand based on public consultation & feedback

Proposed Reactive Services



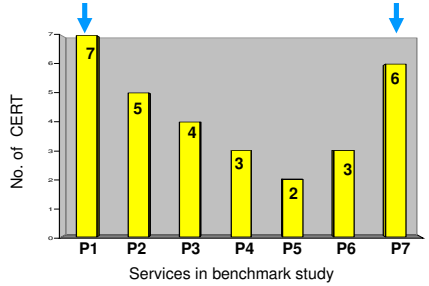
Reactive Services
R1 - Alerts and Warning
R2 - Incident Handling
R3 - Vulnerability Handling
R4 - Artifacts Handling

R1 – **Alerts & Warning** to disseminates information on security issues

R2 – **Incidents Handling** to receive, sort, categorize, prioritize, analyze and document incidents – Response and Handling will be pushed to later phases of project

R3 - **Vulnerability Handling** to receive information about vulnerabilities, analyze and recommend mitigation strategies

Proposed Proactive Services

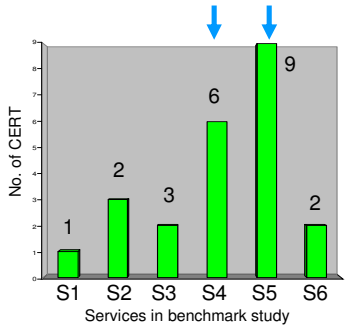


Proactive Services
P1 - Announcement
P2 - Technology Watch
P3 - Security Audit or Assessment
P4 - Configuration & Maintenance of Security Tool, applications & Infra
P5 - Development of Security Tools
P6 - Intrusion Detection Services
P7 - Security Related Information Dissemination

P1 – **Announcements** to focus on medium to long-term impact issues, such as newly found vulnerabilities or intruder tools

P7 - **IT security Information Dissemination** to provides a comprehensive and easy-to-find collection of useful information that aids in improving security

Proposed Security Quality Management Services



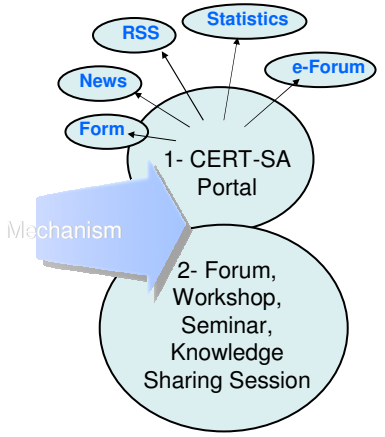
Security Quality Management Services
S1 - Risk Analysis
S2 - Business Continuity & DRP
S3 - Security Consulting
S4 - Awareness Building
S5 - Education/Training
S6 - Product Evaluation or Certification

S4 - **Awareness Building** to provide security awareness program to the constituent to improve their understanding in related security issues

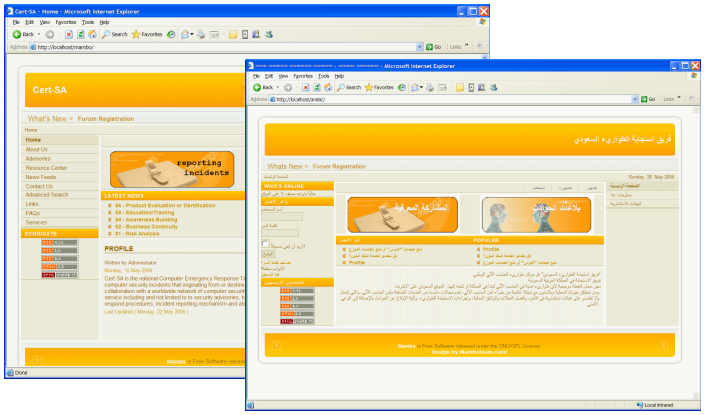
S5 - **Education & Training** through organizing and promoting seminars, workshops, courses, and tutorials.

Service Delivery Mechanism

- R1 – Alerts & Warning
- R2 – Incident Reporting& documentation
- R3 – Vulnerability Handling: Disseminate of known vulnerabilities
- P1 - Announcement
- P7 – Information Dissemination
- S4 – Awareness Building
- S5 – Education/Training



Portal Prototype



Conclusion & Next Steps

Conclusion

- CERT-SA framework development is based on a structured methodology driven by:
  - **International Benchmark study,**
  - **KSA study**
  - **National Information & Communication Plan**
  - **Public specialized opinion (Your valuable input!)**
- Proposed services will be offered in a gradual manner to ensure quality of service, with clear growth path
- To move forward, we need your
  - **Feedback, Support, and Cooperation to strengthen up the foundation of CERT-SA**
- We look forward for many meetings like this to share information and best practice

Next Steps

- Concluding CERT-SA framework development
- Preparing an action plan
- Beginning the Implementation phase
- Counting on your useful feed back and contributions
- Hoping for strong and close cooperation with our partners and constituents

شكرا على حسن استماعكم

WWW. CITC.GOV.SA

Thank You