Strategy to Secure Singapore's Cyber Space

Presented by
Infocomm Security & Assurance Division (ISEC), IDA

iDA SINGAPORE

Agenda

1. Infocomm Security Masterplans
2. Key Highlights
3. Critical Success Factors
4. Moving Forward
   - “Balancing Promote & Protect”

iDA SINGAPORE

Infocomm Security Masterplans

iDA SINGAPORE

Collaborative Approach at Strategic Level

National-level infocomm security programmes driven and led by Government

- National Infocomm Security Committee (NISC)

Partnership between Government, businesses & the people

- Education & information sharing to raise awareness and encourage adoption

International collaborations

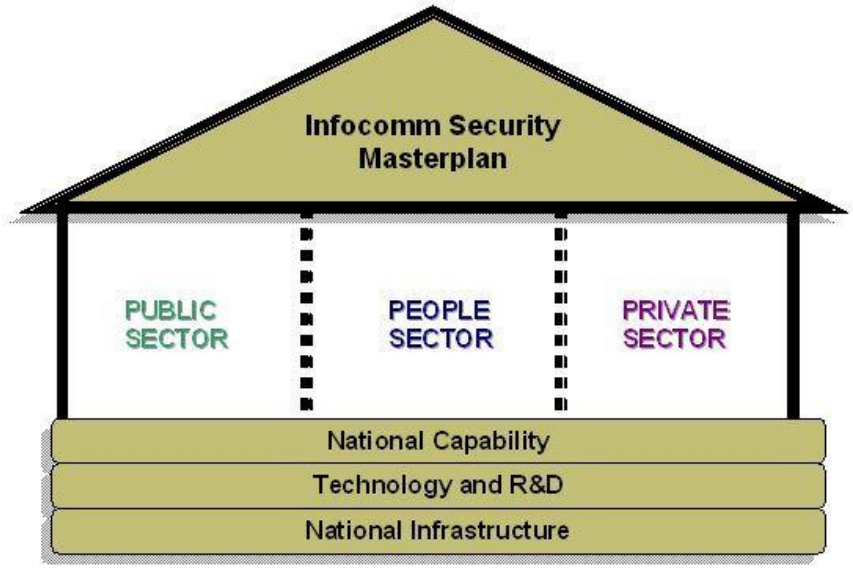
iDA SINGAPORE

Infocomm Security Masterplans

First Masterplan launched in 2005

Objectives:

- Defend Singapore's critical infrastructure from cyber attacks
- Maintain a secure & trusted infocomm environment for the government, businesses and individuals



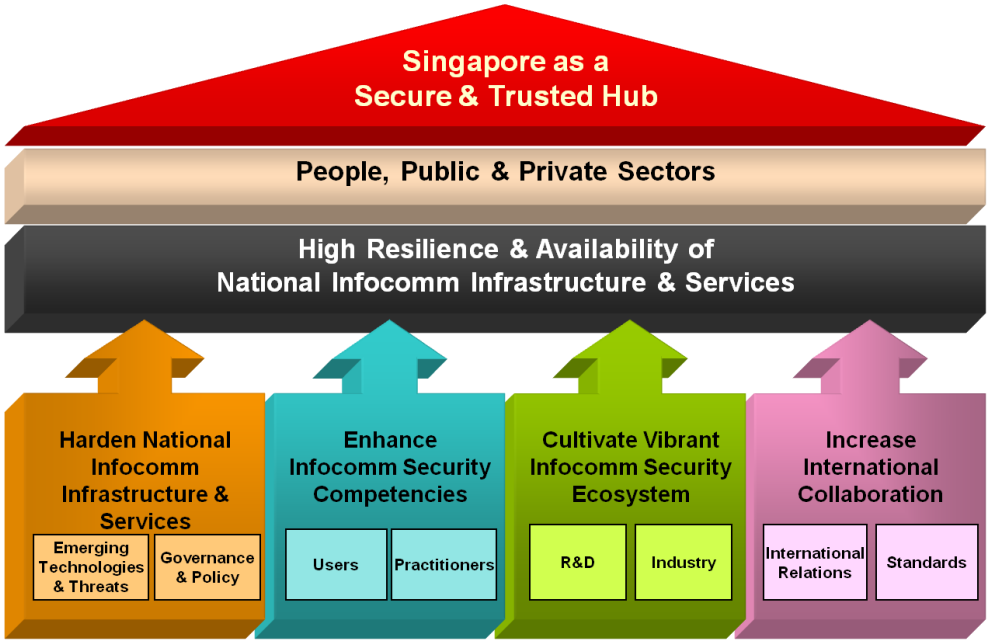
iDA SINGAPORE

Infocomm Security Masterplan 2 (MP2)

5-year Masterplan from 2008 to 2012

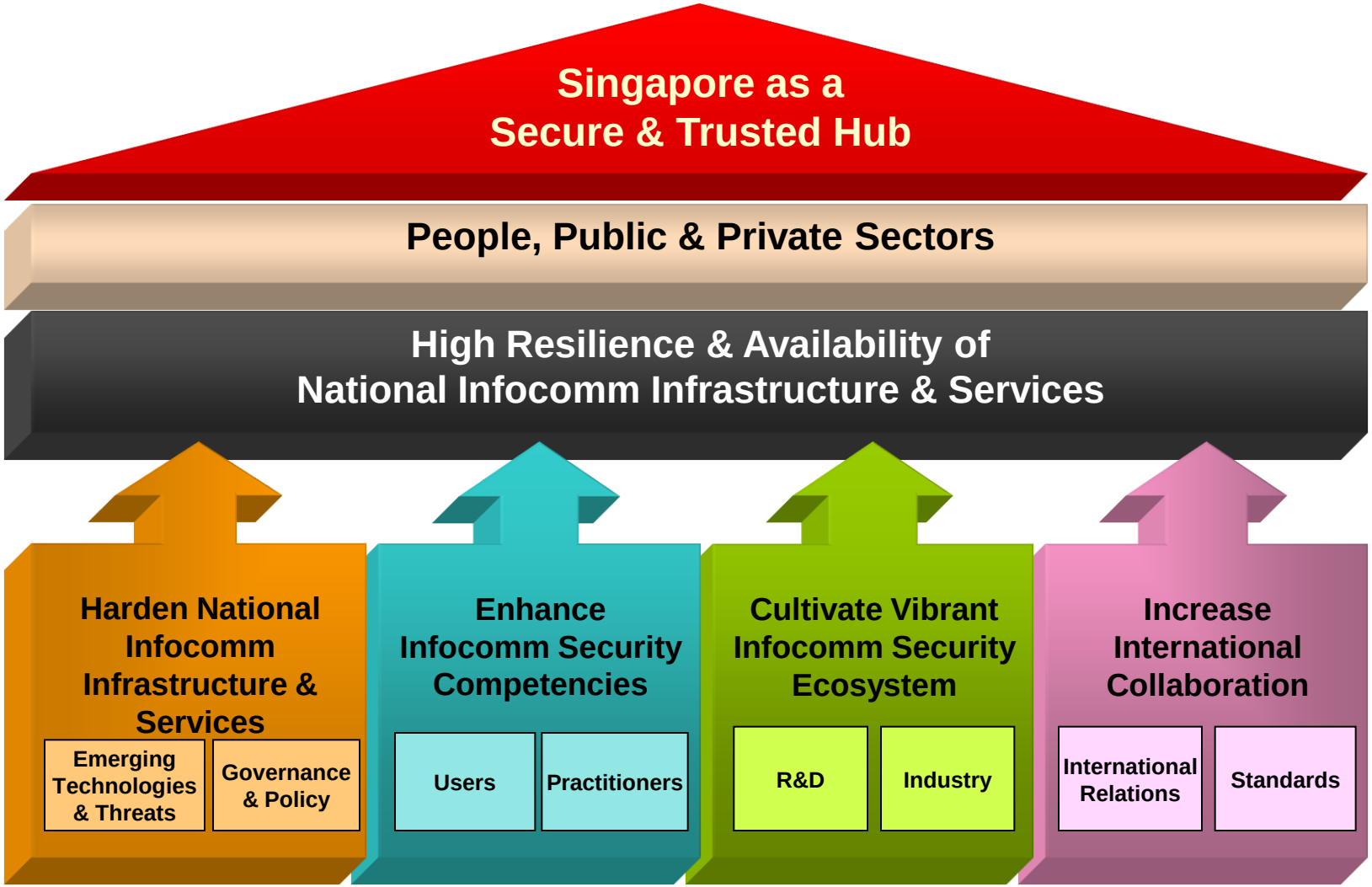
Strategic drivers

1. **Emerging technologies**
   Change in how info services provisioned & consumed
2. **Evolving threats**
   Advanced Persistent Threats (APT) & DDoS Attacks on countries
3. **Borderless cyber threats**
   Common challenge for countries around the world
4. **Engendering confidence**
   Use infocomm security as a strategic business enabler



iDA SINGAPORE

MP2 Framework



iDA SINGAPORE

MP2 Framework - Strategic Thrust 1

Harden national infocomm infrastructure and services

- Vital that Singapore's **national infocomm infrastructure and services are "hardened"** against emerging threats since they form the foundation layer for other services and sectors.

- As such, programmes under this strategic thrust aim to enhance the resilience of our underlying foundation to combat cyber threats.

iDA SINGAPORE

MP2 Framework - Strategic Thrust 2

Enhance infocomm security competencies

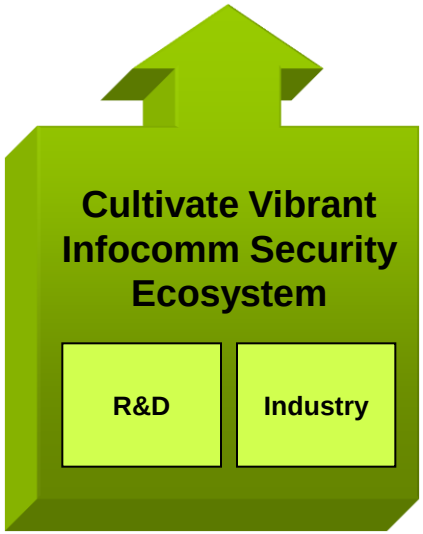
- Looks at enhancing **security competencies** of infocomm **users and infocomm security practitioners.**
- To catalyse **greater adoption of essential security practices** among infocomm users and
- To ensure that infocomm security practitioners have **adequate knowledge and capability in managing infocomm security risks**.

iDA SINGAPORE

MP2 Framework - Strategic Thrust 3

Cultivate vibrant infocomm security ecosystem

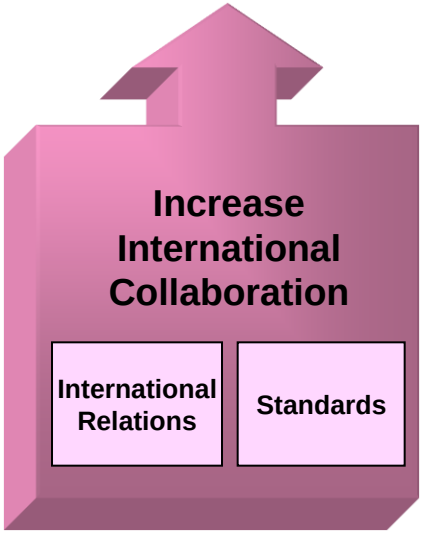
- The presence of a vibrant infocomm security ecosystem strengthens Singapore's capability to protect our national infocomm infrastructure and services.
- An active **infocomm security research and development** scene is helping to ensure that a variety of **up-to-date infocomm security solutions are available** to counter constantly evolving infocomm security threats.



MP2 Framework - Strategic Thrust 4

Increase international collaboration

- Given the borderless nature of cyber threats, it is therefore important to continue to **work closely with our international counterparts**.
- MP2 also focuses on **exchanging best practices** in infocomm security, and **exploring collaborations** in this area.

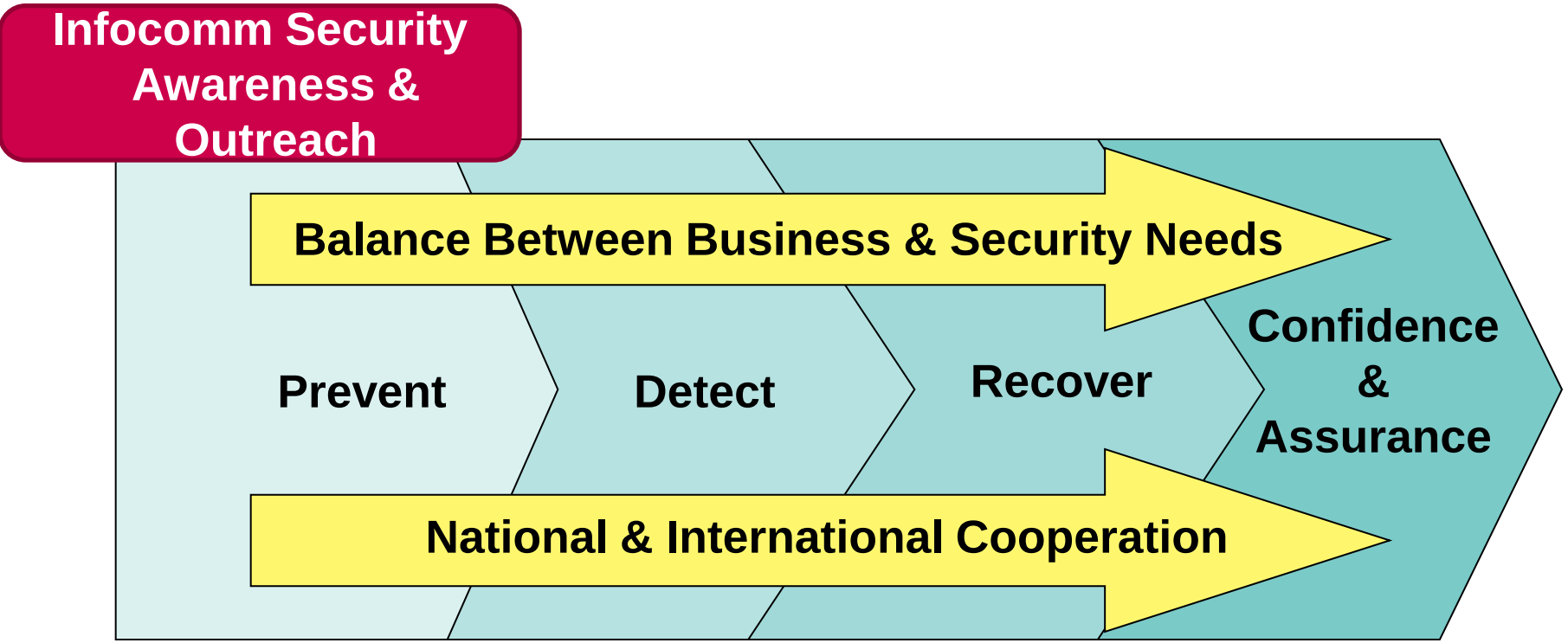


iDA SINGAPORE

Key Highlights

iDA SINGAPORE

Key Highlights



iDA SINGAPORE

Infocomm Security Awareness & Outreach

Cultivate a positive culture of cyber security in Singapore

- Public, Private and People Sectors

Enhance awareness and adoption

Advocate essential cyber security practices

Collaboration through the ‘Cyber Security Awareness Alliance’

Prevent

iDA SINGAPORE

Cyber Security Awareness Alliance

One of the key initiatives under Infocomm Security Masterplan 2

The aim of the Alliance is to:

- Build a positive culture of cyber security in Singapore where infocomm security becomes second nature for all infocomm users; and
- Promote and enhance awareness and adoption of essential infocomm security practices for the Private and People sectors.

Prevent

iDA SINGAPORE

Cyber Security Awareness Alliance

Alliance Partners

iDA SINGAPORE

Private and People Sectors' Initiatives

Alliance-led Efforts

The following **four thrusts** were identified to drive the Alliance's effort to raise awareness and adoption of essential cyber security practices:

Reaching out to the students

Engage youth through a familiar, fun and educational platform

(i.e. Virtual Cyber Security Park)

Reaching out to the Community

Leverage popular networking platforms to reach out to community at large
(i.e. social networking platform)

Cyber Security Outreach

Organise and sponsor events such as seminars, talks, road shows and training workshops

Building the Alliance Brand

Build up brand name and mind share of the infocomm security awareness portal (gosafeonline)

IDA SINGAPORE

Major Milestones for 2011

Information Security Seminar 2011

- More than **400 participants** from public and private sectors
- Student seminar was attended by more **200 students** from various institutes of higher learning

Inaugural Cyber Security Awareness Day

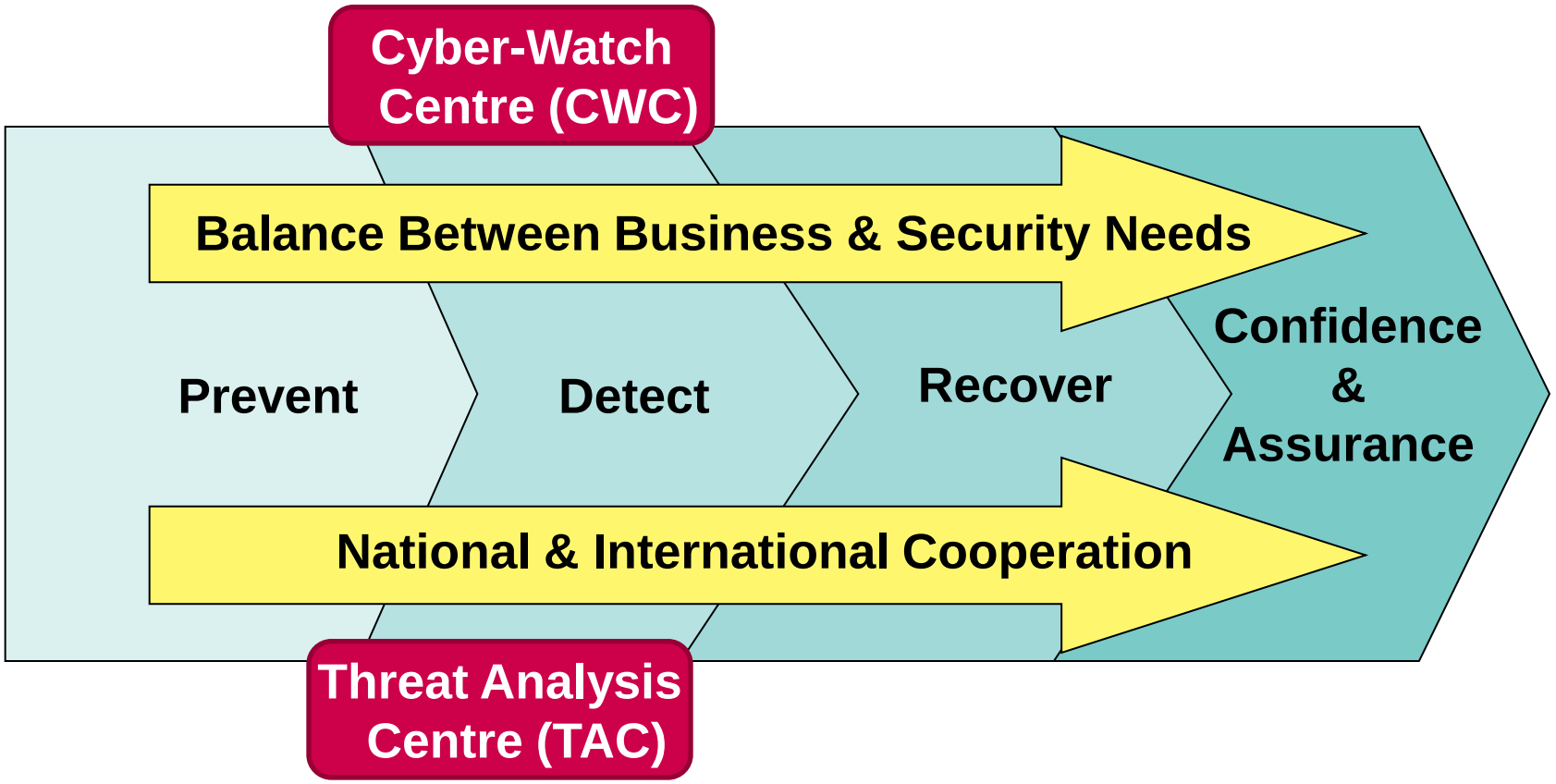
- Launched on **13 April 2011**
- Achieved **307,010** pledge count from public and private sectors, for the call-to-action on the adoption of stronger passwords.
- Media coverage by major newspapers (e.g. The Straits Times, Business Times, etc)

Online Presence

- Launched Cyber Security Awareness Alliance Facebook page
- Launch of Cyber Security Awareness Alliance Web Portal (Articles and resources for Internet users, Parents, Students, SMEs, Senior Citizens)

iDA SINGAPORE

Highlights of Initiatives



iDA SINGAPORE

Cyber-Watch Centre & Threat Analysis Centre

Cyber-Watch Centre (CWC)

- Ongoing round-the-clock security monitoring
- Provides pre-emptive alerts
- Monitors cyber-threats on a real-time basis

Threat Analysis Centre (TAC)

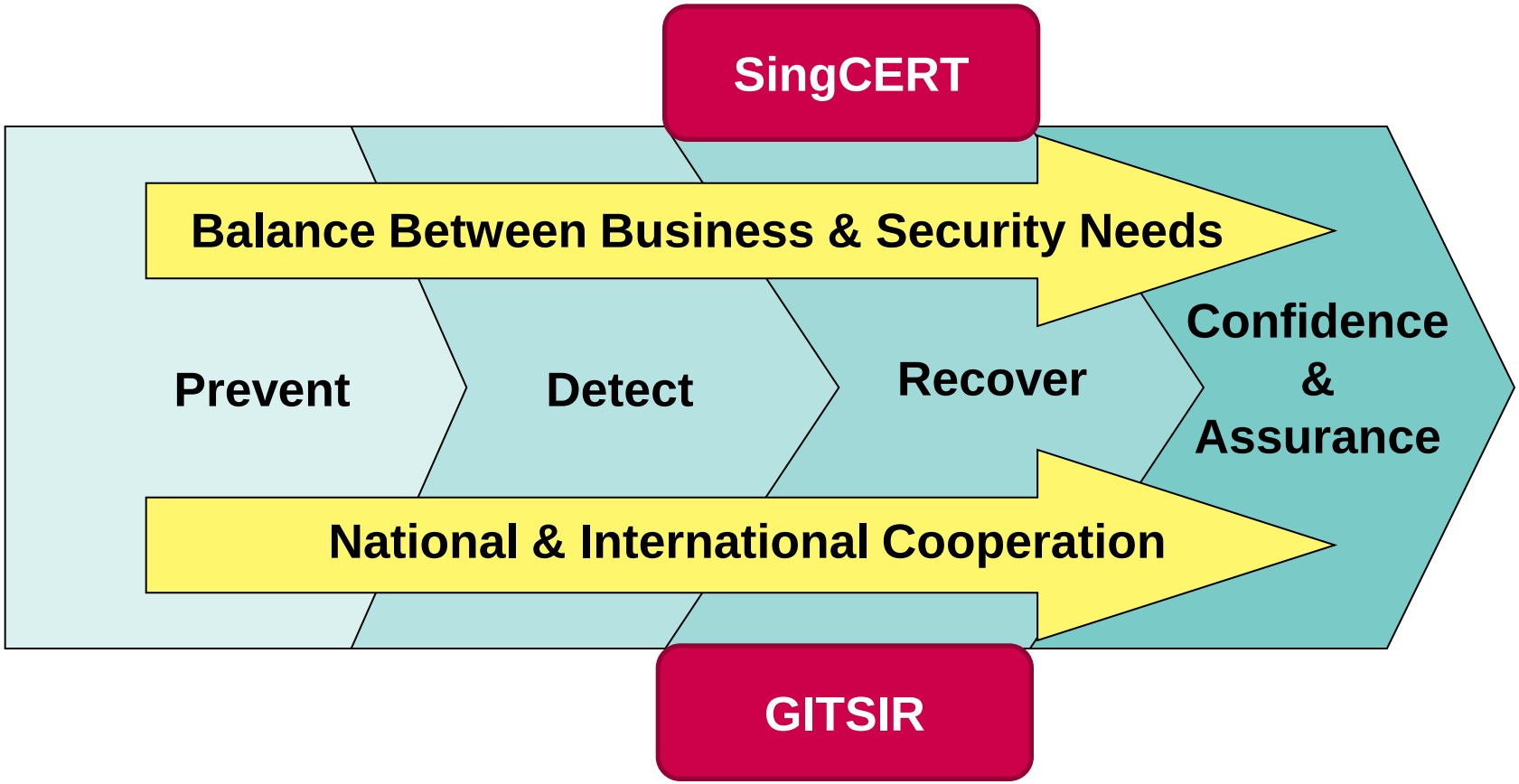
- Ongoing analysis of information
- Monitors cyber threats over the longer term
- Identifies trends

Improves state of security health and help to reduce the occurrences of security incidents

Detect

iDA SINGAPORE

Highlights of Initiatives



iDA SINGAPORE

Security Incident Response & Management

Singapore Computer Emergency Response Team (**SingCERT**) - assistance to businesses and individuals

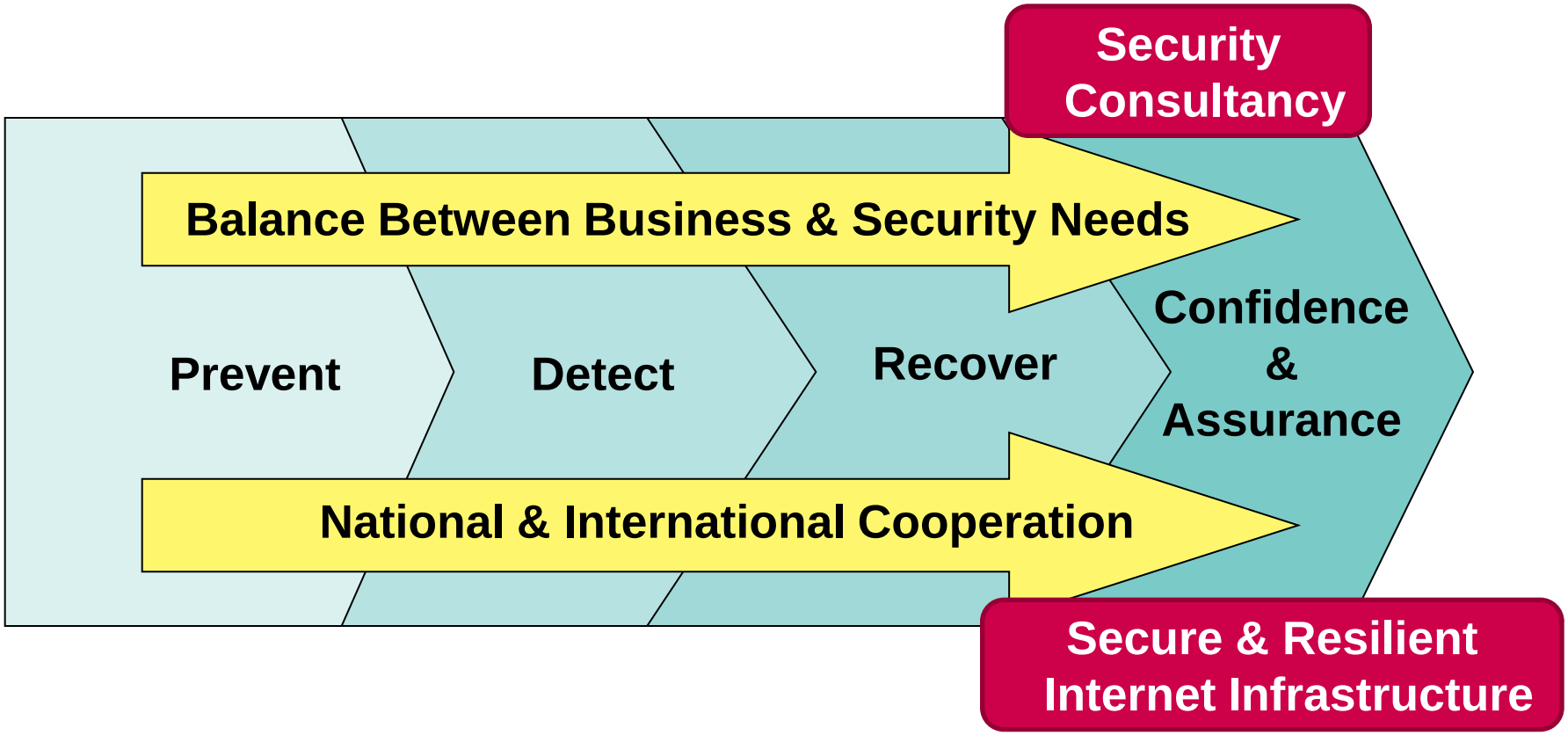
Singapore Govt IT Security Incident Response (**GITSIR**) – assistance to government

- Capability to respond effectively to security incidents
- Coordinate efforts to respond and recover from major security outbreak

Recover

iDA SINGAPORE

Highlights of Initiatives



iDA SINGAPORE

Security Consultancy

Government Service-Wide Projects

National/Cluster-wide projects

Determine & Assess the security requirements, design & implementation

Key Projects

- APEC 2009
- Youth Olympic Games (YOG)
- Next Generation National Broadband Network (NGNBN)
- Government service-wide systems

Assure

iDA SINGAPORE

Secure & Resilient Internet Infrastructure

The programme articulates security requirements for Internet Service Providers (ISP) in providing quality internet services

Issuance of **Code of Practice** to designated Internet Service Providers in February 2011

- Mandates ISPs to develop new capabilities to manage current and emerging cyber threats by ensuring that the right processes are in place.
- ISPs are required to participate in information sharing, which will allow them to adapt their defences accordingly.

Assure

iDA SINGAPORE

Critical Success Factors

iDA SINGAPORE

Critical Success Factors

Endorsement by Top Leadership

- Guidance by senior members of civil service

Partnership

- Engage key players in dialogue – sector leads / regulators, CI owners
- Engage management on the “why”, working-level on the “how”
- Seek collaboration from private sector; use regulator powers only where necessary

Sufficient Resources

- Right people, business partners
- Central seed funding

iDA SINGAPORE

Moving Forward

iDA SINGAPORE

Emerging Technologies

- Change in how info services provisioned & consumed
  - E.g. Mobile devices have radically changed accessibility of sensitive data outside an organisation's walls
  - E.g. Convergence of multiple functional systems onto common IP-based infrastructure
- Tablets, Smart phones, Cloud computing, Web 2.0, etc
  - E.g. Utilisation of shared app, storage resources through virtualisation and cloud computing
- Workplace of the Future for Government

iDA SINGAPORE

Evolving Threats

- Advanced Persistent Threats (APT)
  - E.g. high-profile targeted attacks: “Shady RAT”, U.N., U.S. defence contractors, Google, RSA, Sony, G20
- Distributed Denial-of-Service (DDoS) attacks
  - E.g. Malaysia, U.S., South Korea, Estonia, Georgia.
- “Cyber Hooligans” / Cyber Crime
  - E.g. website defacements, phishing for personal information

“Balancing Promote & Protect”

iDA SINGAPORE

Thank you

iDA SINGAPORE