Case Study on National Cybersecurity Strategy: Qatar

19 February 2008

Steve Huth
Director, Q-CERT
shuth@qcert.org

I: Developing and Obtaining Agreement on a National Cybersecurity Strategy

- Developing and implementing a national cybersecurity plan requires a comprehensive strategy that includes an initial broad review of the adequacy of current national practices and consideration of the role of all stakeholders (government authorities, industry, and citizens) in the process. [1]

[1] ITU STUDY GROUP Q.22/1 REPORT ON BEST PRACTICES FOR A NATIONAL APPROACH TO CYBERSECURITY: A MANAGEMENT FRAMEWORK FOR ORGANIZING NATIONAL CYBERSECURITY EFFORTS – Draft January 2008

Link Strategy to National Vision

- His Highness the Emir established ictQATAR in 2004
- ictQATAR: We *connect* people to the technologies that will *enrich* their lives, drive economic development and *inspire* confidence in our nation's future
- This requires secure, resilient information and communication technology
- Q-CERT began operation in 2006

Q-CERT Strategic Plan

- Created by Carnegie Mellon as part of the plan for Q-CERT
- Strategic Plan Includes
    - Planning, Measurement, and Evaluation
    - Deterrence
    - Protection
    - Monitoring, Detection, and Analysis
    - Response
    - Reconstitution and Recovery
    - Research and Development

Developing and Obtaining Agreement on a National Cybersecurity Strategy

- Create awareness at a national policy level about cybersecurity issues and the need for national action and international cooperation.
- Develop a national strategy to enhance cybersecurity to reduce the risks and effects of both cyber and physical disruptions.
- Participate in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents.

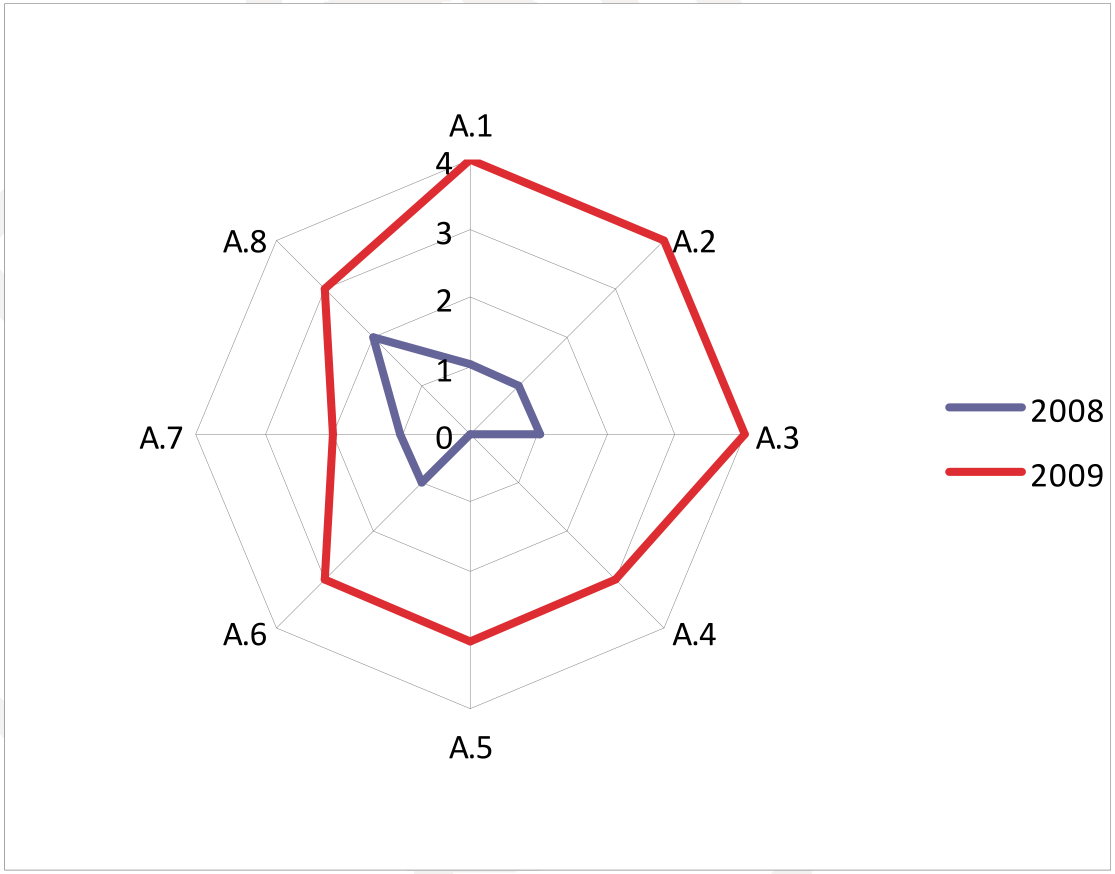
Specific Steps

- Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the national cyber infrastructure through policy-level discussions.
- Identify a lead person and institution for the overall national effort; determine where within the government a Computer Security Incident Response Team with national responsibility should be established; and identify lead institutions for each aspect of the national strategy.
- Identify the appropriate experts and policymakers within government ministries, government, and private sector, and their roles.
- Identify cooperative arrangements for and among all participants.
- Establish mechanisms for cooperation among government and private sector entities at the national level.
- Identify international expert counterparts and foster international efforts to address cybersecurity issues, including information sharing and assistance efforts.
- Establish an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity.
- Assess and periodically reassess the current state of cybersecurity efforts and develop program priorities.
- Identify training requirements and how to achieve them.

Use the Framework as a Way of Discussing Strategy

✓	**I. National Strategy** ▪ Create awareness at national policy level about cybersecurity and the need for national action and international cooperation. ▪ Develop a national strategy to enhance cybersecurity to reduce the risks and effects of cyber disruptions. ▪ Participate in international efforts for the prevention of, preparation for, preparation for, response to, and recovery from incidents.
✓	**II. Government-Industry Collaboration** ▪ Develop government-industry collaborations that work to effectively manage cyber risk and to protect cyberspace. ▪ Provide a mechanism for bringing a variety of perspectives, equities, and knowledge together to reach consensus and move forward together to enhance security at a national level.
?	**III. Deterring Cybercrime** ▪ Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent with the provisions of the Convention on Cybercrime (2001).
✓ ✓ ✓ ✓	**IV. Incident Management Capabilities** ▪ Develop a coordinated national cyberspace security response system to prevent, detect, deter, respond to and recover from cyber incidents. ▪ Establish a focal point for managing cyber incidents that bring together critical elements from government (including law enforcement) and essential elements from infrastructure operators and vendors to reduce both the risk and severity of incidents. ▪ Participate in watch, warning and incident response information sharing mechanisms. ▪ Develop, test and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.
✓	**V. Culture of Cybersecurity** ▪ Promote a national Culture of Security consistent with UNGA Resolutions 57/239, Creation of a global culture of cybersecurity, and 58/199, Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

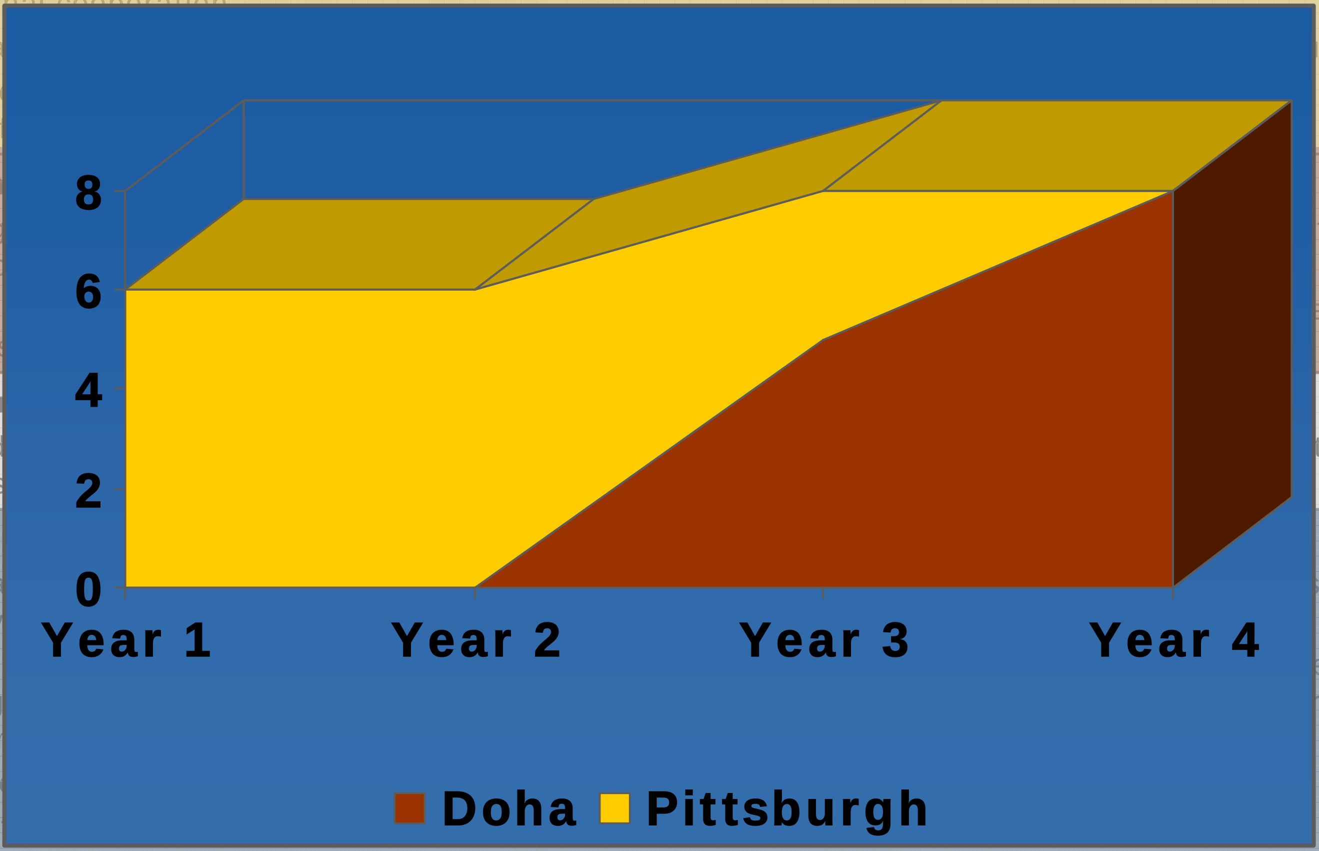
The Self-Assessment Toolkit



Map Capabilities onto the Framework

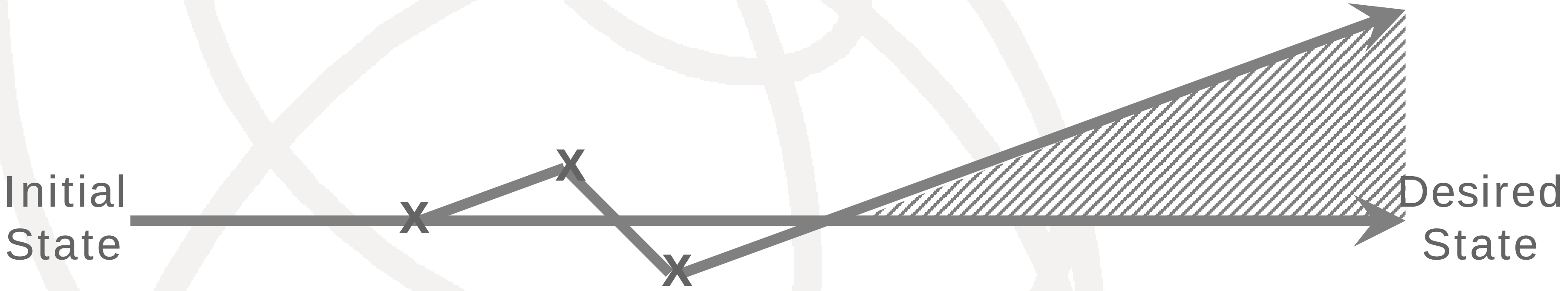
Director's Office	**I. National Strategy** ▪ Create awareness at national policy level about cybersecurity and the need for national action and international cooperation. ▪ Develop a national strategy to enhance cybersecurity to reduce the risks and effects of cyber disruptions. ▪ Participate in international efforts for the prevention of, preparation for, preparation for, response to, and recovery from incidents.
CIP	**II. Government-Industry Collaboration** ▪ Develop government-industry collaborations that work to effectively manage cyber risk and to protect cyberspace. ▪ Provide a mechanism for bringing a variety of perspectives, equities, and knowledge together to reach consensus and move forward together to enhance security at a national level.
	III. Deterring Cybercrime ▪ Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent with the provisions of the Convention on Cybercrime (2001).
Incident Management	**IV. Incident Management Capabilities** ▪ Develop a coordinated national cyberspace security response system to prevent, detect, deter, respond to and recover from cyber incidents. ▪ Establish a focal point for managing cyber incidents that bring together critical elements from government (including law enforcement) and essential elements from infrastructure operators and vendors to reduce both the risk and severity of incidents. ▪ Participate in watch, warning and incident response information sharing mechanisms. ▪ Develop, test and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.
OA&T	**V. Culture of Cybersecurity** ▪ Promote a national Culture of Security consistent with UNGA Resolutions 57/239, Creation of a global culture of cybersecurity, and 58/199, Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

And Develop Metrics to Measure Progress

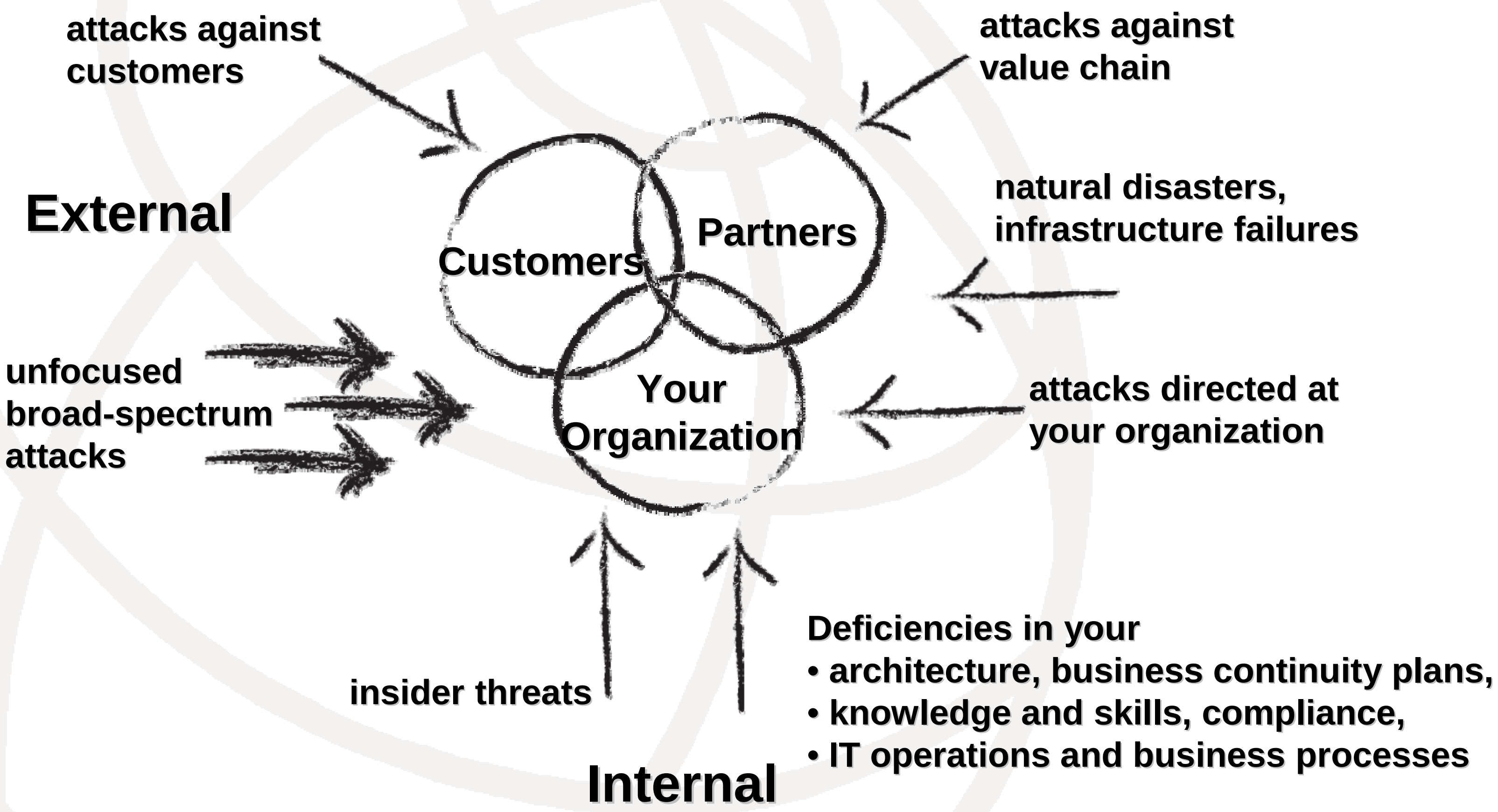


Director's Office	**I. National Strategy** ▪ Create awareness at national policy level about cybersecurity and the need for national action and international cooperation. ▪ Develop a … ptions. ▪ Participat … to, and recovery f …
CIP	**II. Govern …** ▪ Develop g … tect cyberspac … ▪ Provide a … each consensus …
	III. Deter … ▪ Enact and … t with the provis …
Incident Management	**IV. Incide …** ▪ Develop a … spond to and recov … ▪ Establish … ernment (including … reduce both the r … ▪ Participate … ▪ Develop, … government and non-government collaborators can build trust and coordinate effectively in a crisis.
OA&T	**V. Culture of Cybersecurity** ▪ Promote a national Culture of Security consistent with UNGA Resolutions 57/239, Creation of a global culture of cybersecurity, and 58/199, Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

Flexible Strategy



What does the world look like to you?



attacks against customers

attacks against value chain

External

Customers

Partners

Your Organization

natural disasters, infrastructure failures

unfocused broad-spectrum attacks

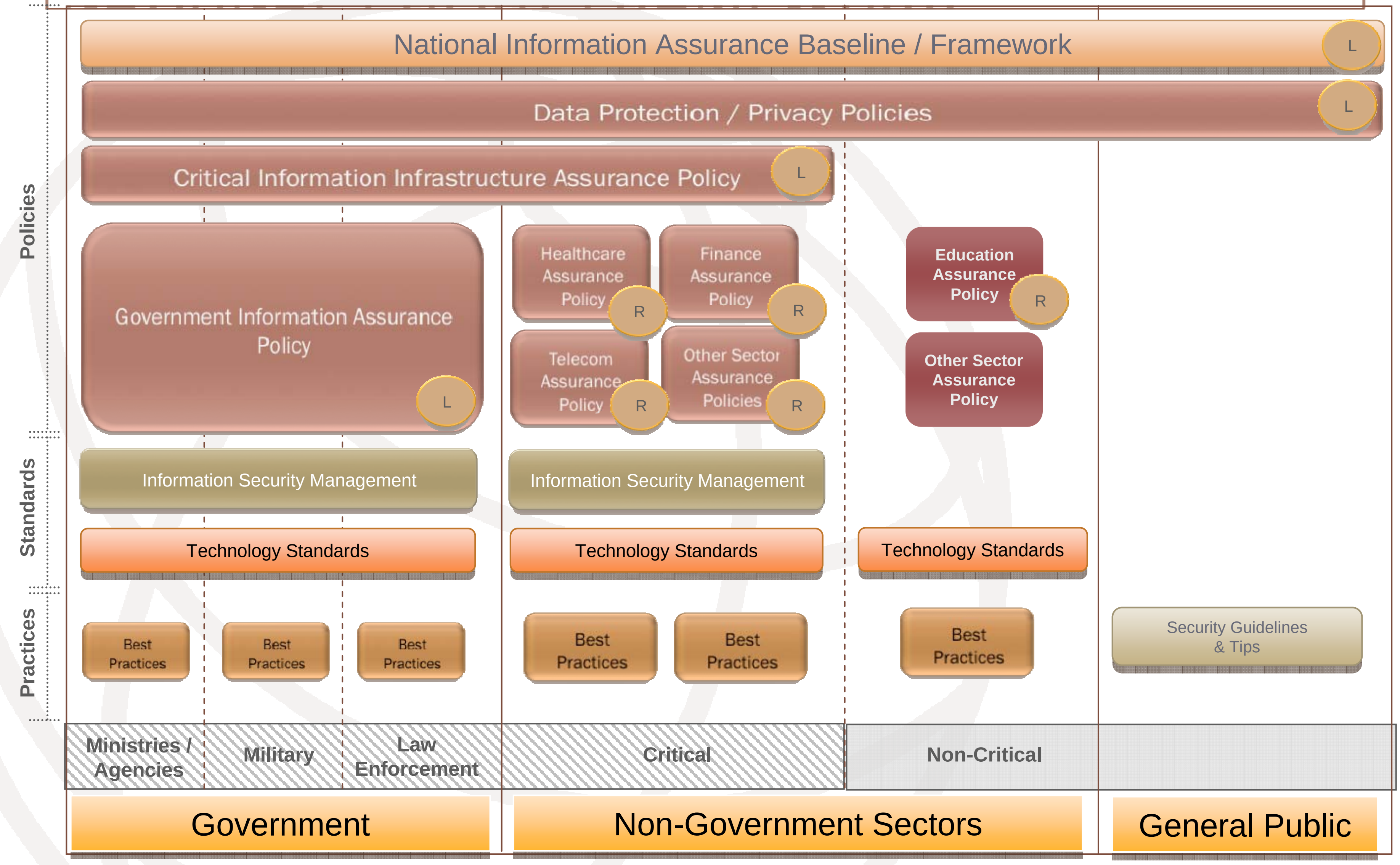
attacks directed at your organization

insider threats

Deficiencies in your
- architecture, business continuity plans,
- knowledge and skills, compliance,
- IT operations and business processes

Internal

NATIONAL POLICY FRAMEWORK



Policies

Standards

Practices

National Information Assurance Baseline / Framework L

Data Protection / Privacy Policies L

Critical Information Infrastructure Assurance Policy L

Government Information Assurance Policy L

Healthcare Assurance Policy R

Finance Assurance Policy R

Telecom Assurance Policy R

Other Sector Assurance Policies R

Education Assurance Policy R

Other Sector Assurance Policy

Information Security Management

Information Security Management

Technology Standards

Technology Standards

Technology Standards

Best Practices

Best Practices

Best Practices

Best Practices

Best Practices

Best Practices

Security Guidelines & Tips

Ministries / Agencies

Military

Law Enforcement

Critical

Non-Critical

Government

Non-Government Sectors

General Public

L Mandatory by Legislation

R Mandatory by Regulation

Additional Lessons Based on Our Experiences

- Champion with high-level access
- Formal national strategy doesn’t have to come first
- Identify and understand your constituents
- Partnerships
- Discussion are as important as the outcome
- Small wins / incremental gains
- Culture
- Build trust
- National strategy for an international problem
- Keep it simple
- Be able to answer the question
  “How does this improve the lives of our citizens?”
- Think broadly

Conclusion

- This is all obvious in hindsight
- The Cybersecurity Framework and related tools give you a way of thinking through the issues related to your national strategy
- Strategy and tools are worthless...

...without good people