Q-CERT

“A National CERT – what can it do for you?”

Ian M Dowdeswell

Qatar Computer Emergency Response Team (Q-CERT)

Presentation Overview

- Who we are
- What we do
- What we can do for you
- Questions

What is Q-CERT?

- The national computer information security team for the State of Qatar

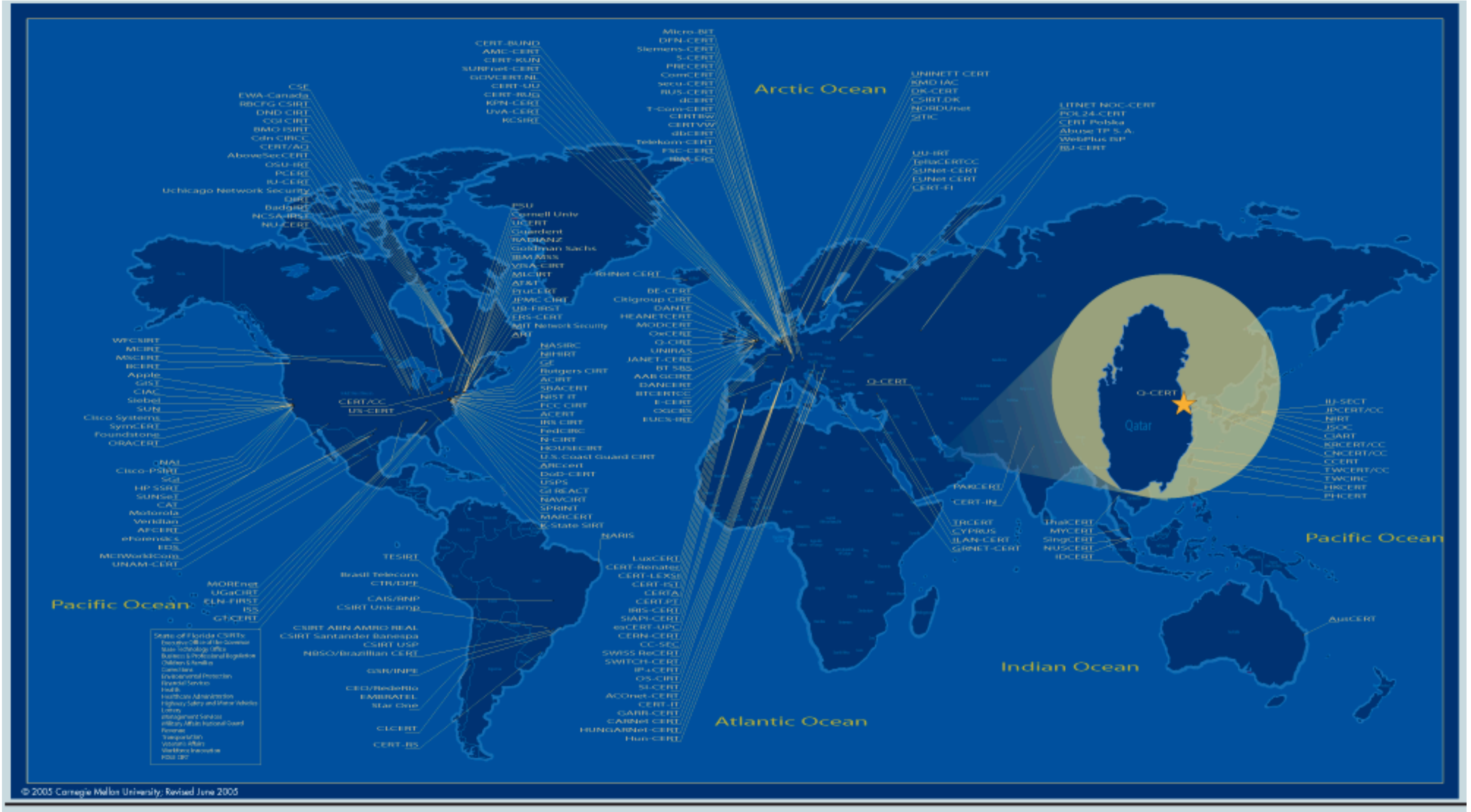
- Works with organizations who deliver critical services in Qatar to help them:
  - identify their most important information assets
  - develop appropriate risk management strategies
  - prevent attacks by improving the security of the services that they provide
  - recognize cyber attacks and respond effectively

Q-CERT

- Helps Critical Sector Organizations
  - to create and improve their cyber security capability and capacity

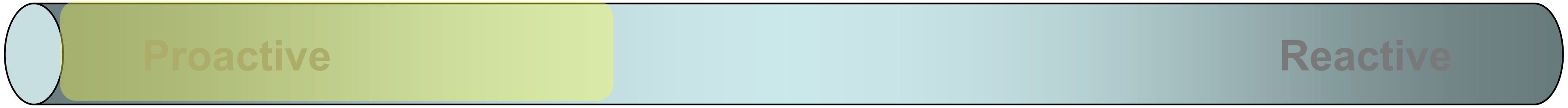
- Works with other security teams world-wide
  - to maintain awareness of global trends
  - to coordinate response to international threats & incidents (as cyber security is not confined to national boundaries)

Q-CERT – Part of the Global Response Network



© 2005 Carnegie Mellon University; Revised June 2005

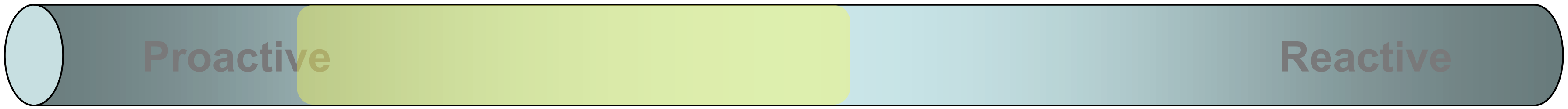
Q-CERT
Range of Activities



Outreach, Awareness, & Training

- Tailored workshops based on needs analysis
- Public workshops based on recognized needs
- Outreach to region

Q-CERT
Range of Activities



Critical Infrastructure Protection

- Assist key national resources in addressing information security vulnerabilities and threats
- Assist in creating an Information Security management framework
- Develop and provide approaches for risk assessments and risk mitigation

Q-CERT
Range of Activities

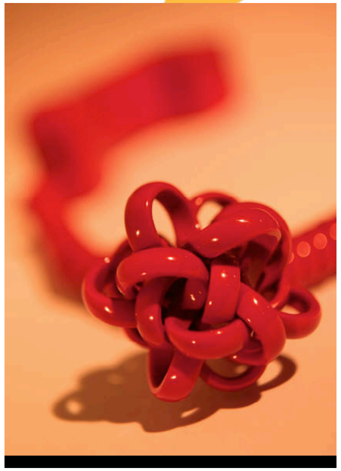
Proactive
Reactive

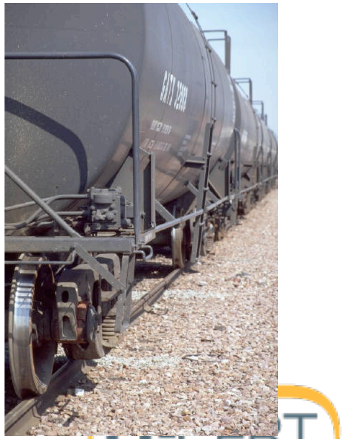
Incident Management

- Establish a national and regional center for threat, vulnerability, and security event data.
- Establish and operate mechanisms for responding to cyber threats and vulnerabilities.
- Assist law enforcement and other responders organizations.

The Threat

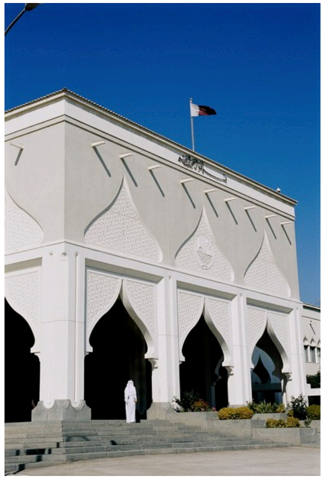
- **Interruption of Telecommunications**
  - Impact on all levels of communications
  - 999 service potentially off line (Cascade effect)
  - Severe impact on financial services
  - Loss of communications with public impacts confidence in government
  - Potentially serious impact on civilian logistics
- **Interruption of Transportation**
  - Disruption of commerce
  - Foodstuffs and fuel deliveries interrupted
  - Potential hazardous material compromises
  - Direct impact on population





The Threat

- **Interruption of Government Services**
  - Loss of public confidence
  - Impact on disaster recovery (Cascade effect)
  - Potential crisis in leadership



- **Interruption of Information Infrastructure**
  - Significant impact on other critical infrastructures
  - E-commerce halted
  - Networks become unreliable
  - Direct impact on population

Emerging Threats

- New Technologies bring New Threats
  - Inherent vulnerabilities with new technology
  - Wireless technologies
    - 802.11X
    - Cell Phones
    - Wireless video
  - Application programs
  - Information storage devices

Incident Management Activities

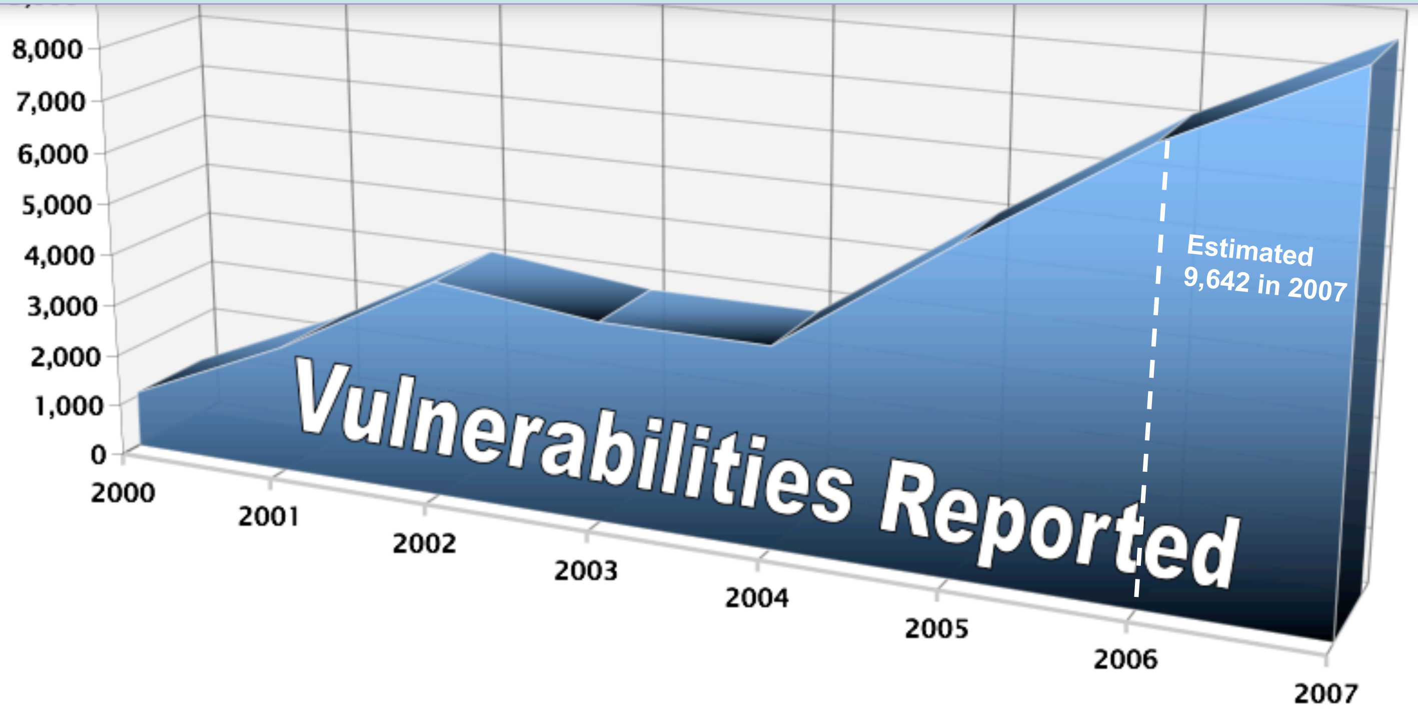
Threat gathering activities

- Honeynet data analysis
- Open- source monitoring
- Netflow data analysis of network traffic flow across national gateways to determine risk to CIP.

Q-CERT

Vulnerability Statistics

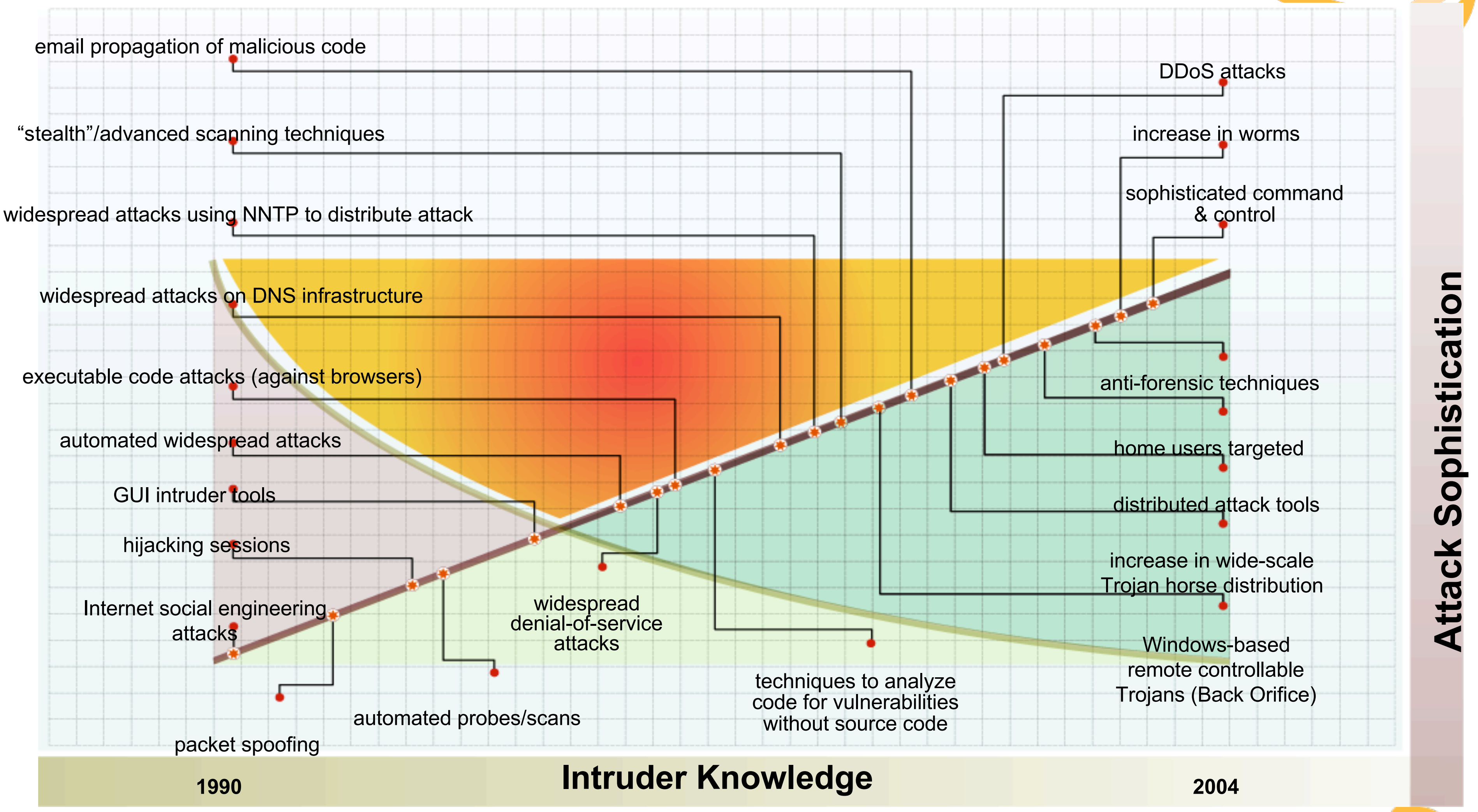
Today CERTCC receives more than 25 vulnerabilities every day



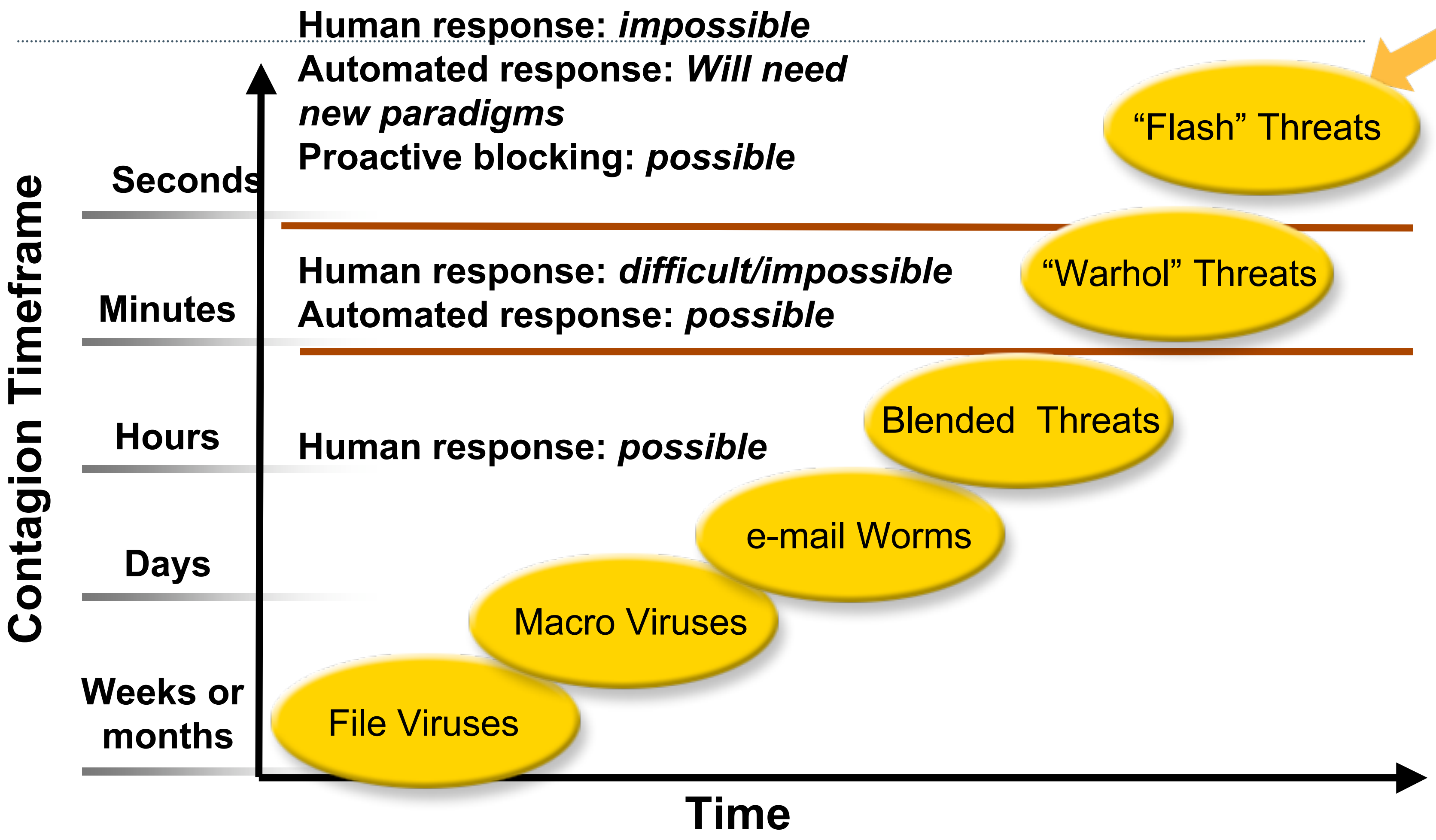
Year	2000	2001	2002	2003	2004	2005	2006	2007
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	8,064	9,642

Note: The number of estimated reports for 2007 is based on the current volume being reported.

Attack Sophistication vs. Intruder Knowledge



IT System Threat Evolution in the Future



Human response: *impossible*
Automated response: *Will need new paradigms*
Proactive blocking: *possible*

Human response: *difficult/impossible*
Automated response: *possible*

Human response: *possible*

Incident Management Activities

Vulnerability information dissemination

- key, relevant information topics, in English and Arabic, for timely dissemination to constituency.
- advice on best sources of vulnerabilities.
- warnings from global partners - no longer a ‘individual contest’.

Critical Infrastructure Defined

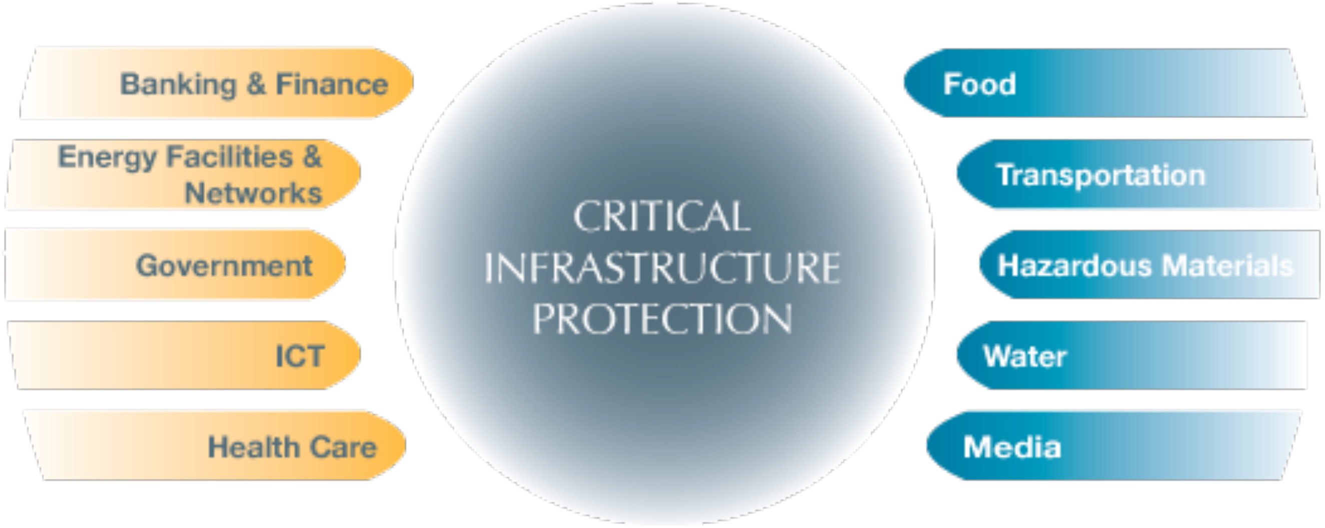
Critical Infrastructure:

- Physical and information technology services and assets which, if disrupted, destroyed or compromised, would have a serious impact on the health, safety, security or economic well-being of Qatar or the effective functioning of its government

- Banking and financial services
- Medical services
- Gas facilities and networks
- Government services

CIP Sectors

Sectors are deemed critical when their incapacitation or destruction would have a debilitating impact on the national security and social well-being of a nation



Sector Security

- Infrastructure Vulnerabilities

- Most Infrastructures are Scale-free networks
  - Able to survive random attacks or failures
  - Highly susceptible to targeted attack
    - Super Hubs (Financial)
    - Considerable redundancy within the system but not *of* the system (Telecommunications)

- Database Compromise
  - Ability to Destroy, Disrupt, or Distort critical data
  - Information as essential as physical infrastructure

- Physical Attack
  - Loss of facilities
  - Redundancy becomes critical

- Combined Physical/Cyber Attack
  - Force multiplier

Critical Sector Organisation (CSO) Engagement

- Reduce information risk in the CSO, hence reduce risk in critical infrastructure
- Help define security strategy & objectives for meeting CSO, regulatory, legislative and government (CIP) requirements
- Help to address CSO's current issues: provide independent consultancy based on best practice
- Provide advice on long term security improvement, with appropriate (holistic) scope & governance
- Provide independent testing and measurement of security improvement over time
- Help CSO to adopt internationally recognised best practices for their sector
- Help Q-CERT understand sector security issues and help raise the levels of practice in the whole sector

Critical Infrastructure Protection Challenge

Cyber space and physical space are becoming one

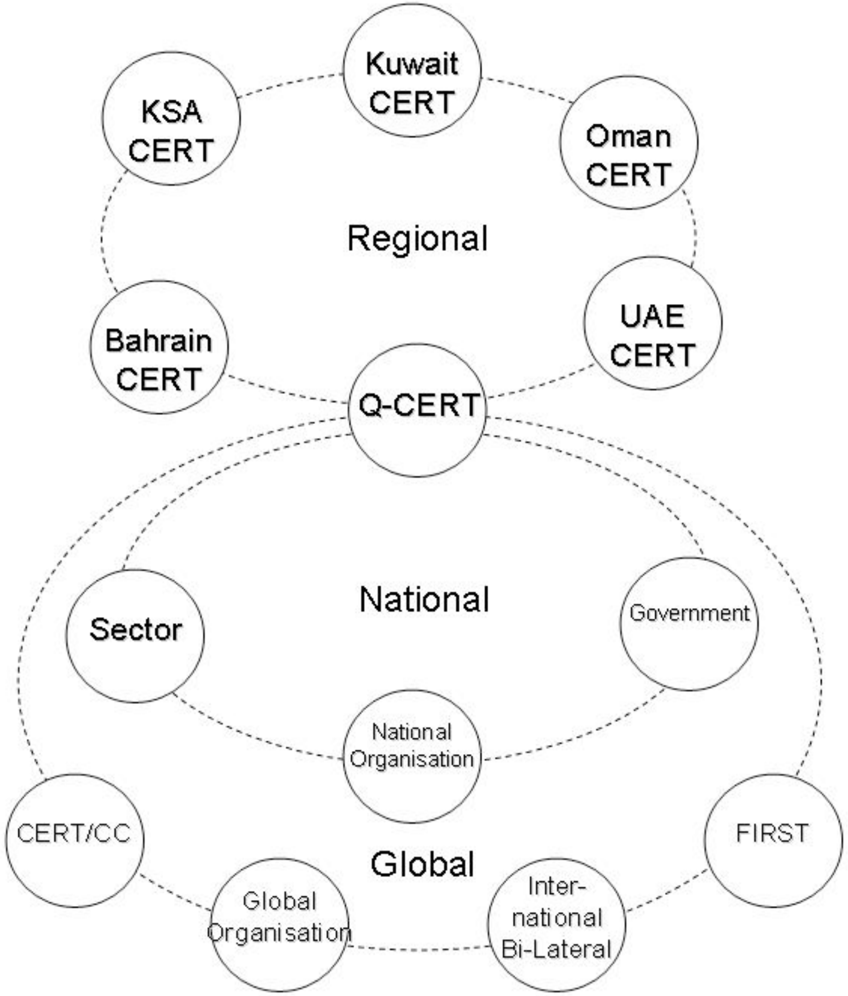
In the U.S. alone:

- Agriculture and Food
  - 1.9M farms
  - 87,000 food processing plants
- Water
  - 1,800 federal reservoirs
  - 1,600 treatment plants
- Public Health
  - 5,800 registered hospitals
- Chemical Industry
  - 66,000 chemical plants
- Telecomm
  - 2 B miles of cable
- Energy
  - 2,800 power plants
  - 300K production sites
- Transportation
  - 120,000 miles of railroad
  - 590,000 highway bridges
  - 2M miles of pipeline
  - 300 ports
- Banking and Finance
  - 26,600 FDIC institutions
- Postal and Shipping
  - 137M delivery sites
- Key Assets
  - 5,800 historic buildings
  - 104 nuclear power plants
  - 80K dams
  - 3,000 government facilities
  - 460 skyscrapers

Regional Cooperation

- The GCC-CERT was established by decision of the Gulf Cooperation Council, as a collaboration amongst the emerging GCC national programs:
  - “GCC council mandates members to expedite the process of establishing their national CERT programs”
- The GCC decision established a framework for regional cooperation amongst Gulf states on the topic of information security.
- Working Group meetings are ongoing to fulfill the GCC instructions – we welcome our GCC colleagues!

Constituency



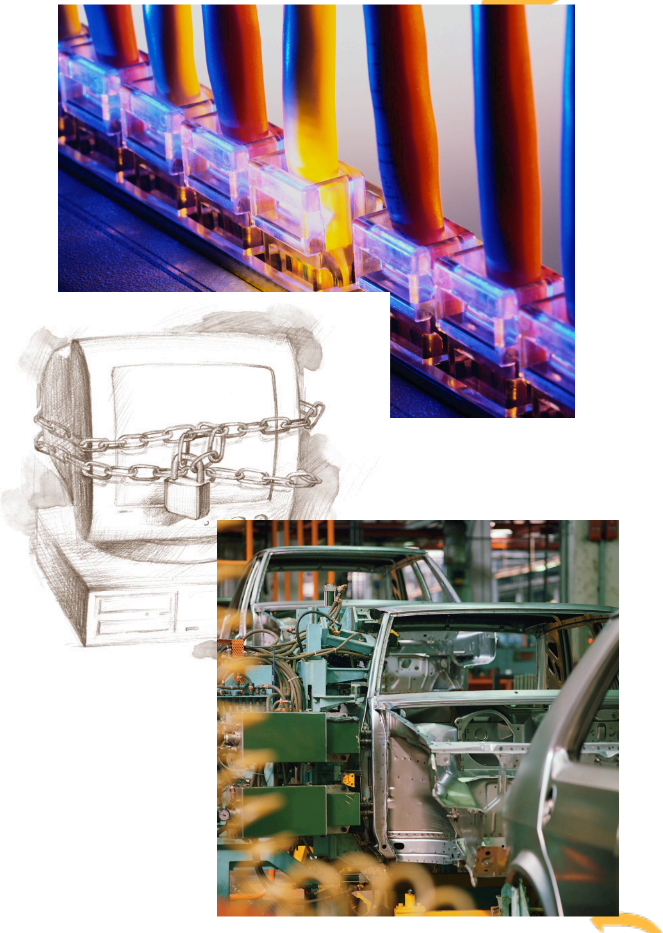
Changing Security Requirements

- Fortress approach no longer viable
  - Risk Management is key
  - What is most important to the organization
  - What is the greatest threat
  - What resources are needed

- Focus is on providing resiliency to the organization
  - Keep it operating if possible
  - If not, prepare for graceful degradation
  - Should stronger/more capable at the end

Changing Security Requirements

- What are the impacts of emerging technologies?
  - What are your vulnerabilities?
  - What do they mean to physical security of the organization?
  - Do you have the expertise necessary to understand and mitigate threats
- What does a technical compromise mean?
  - Halt of production
  - Unauthorized Access
  - Damage
    - Intended
    - Accidental



Challenges

- Integrated Security has to be part of the strategic plan for an organization

- Security strategies must enable the organization, but must be balanced against potentially limiting the achievement of other strategic objectives

In Summary

- Incident Management – for response to and coordination of security incidents of national importance
- Outreach and Awareness – for developing knowledge of and skills in information security
- Critical Infrastructure Protection – for long-term organizational risk assessment and process improvement

Incident Management
Points of Contact

Report Incidents by:

Website (using proforma):
www.qcert.org

Email:
incidents@qcert.org

Phone:
+974 493 3408

Fax:
+974 483 9953

Incident Manager –

Ian M Dowdeswell

imd@qcert.org

Questions?