Q-CERT

Creation of a National Response Team

A case study of Q-CERT

Dr. Rashid al-Ali, Program Managing Director
Archie Andrews, Technical Director
Michael Lewis, Deputy Director

ict قطر QATAR

Oryx

Gazelle of Qatar

Overview

- Motivation for Founding Q-CERT
- Regional Cooperation – the GCC-CERT
- Q-CERT Vision, Relationships, & Activities
- What Have You Done for Qatar Today?
- Observations & Lessons Learned

ictQATAR

- Information Technology is a fundamental component of Qatari national and Gulf regional development
- The Supreme Council of Information Technology of Qatar (ictQATAR) is the premier national body responsible for technology initiatives

ictQATAR Projects

The program includes initiatives such as:

- eHealth
- eGovernment
- eFinance
- eLearning

and many more, ranging from regulatory responsibilities to “Telecom for Life” ...

... all of which require robust and secure computers and network systems.

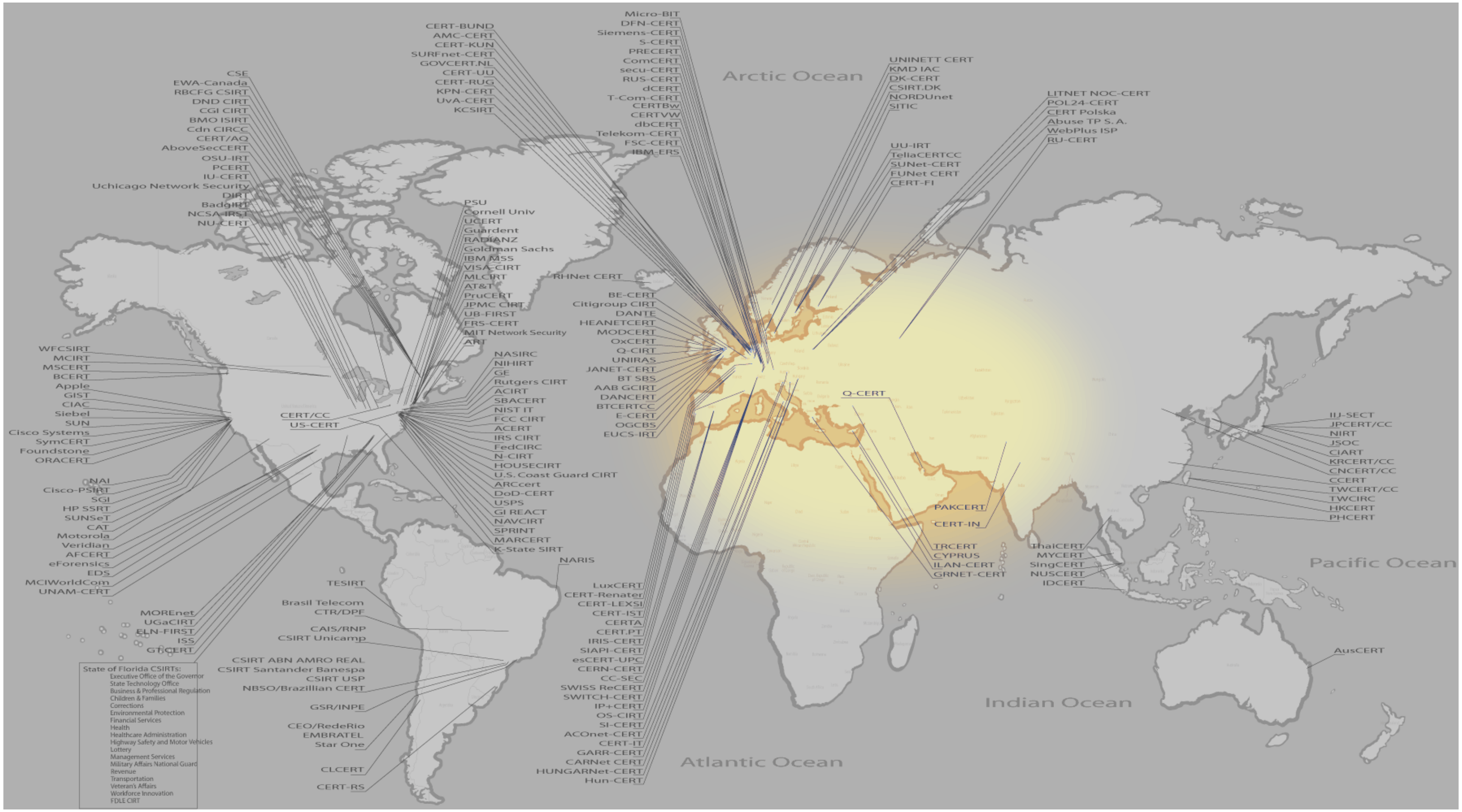
Information Security Message

- Every organization should have a strategy for Information Security.
- A proven approach is to develop a Computer Security Incident Response Team (CSIRT), to formalize and implement the strategy.
- CSIRTs can be internal to a company, to a sector, or have national or regional responsibilities.

A Critical Need

1. There are now CERT/CSIRT programs throughout the world
2. The model has proven to be effective
3. There is a limited presence of such programs in the Middle East

The Global Picture



ictQATAR

- recognized the fundamental role of Information Security for the region
- established a long-term strategic partnership with the CERT/CC
- sponsored the Q-CERT program
- and is the founding partner of the regional GCC-CERT initiative

Regional Cooperation

- The GCC-CERT was established by decision of the Gulf Cooperation Council.
- The GCC decision approved a framework for regional cooperation amongst Gulf states on the topic of information security.

The GCC decision

“GCC council mandates members to expedite the process of establishing their national CERT programs”

Q-CERT:

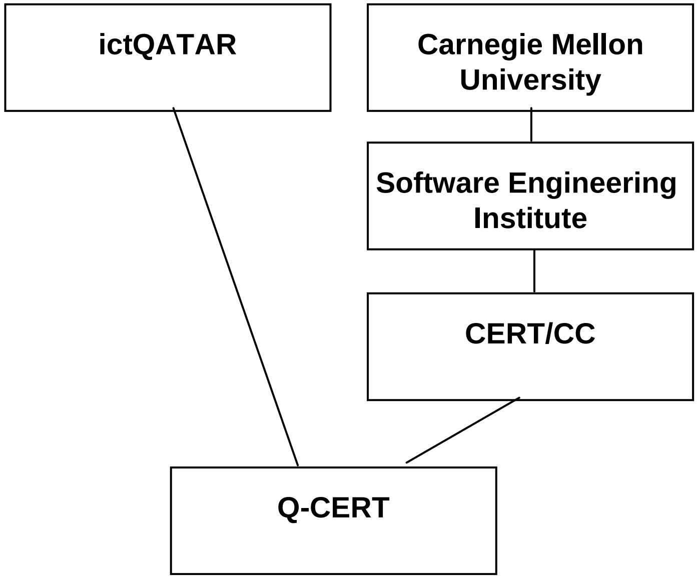
- hosted a regional workshop on Building National CERT programs (June ’06)
- developed the regional framework for cooperation
- is implementing a regional program of training and development for building national CSIRTs

ictQATAR / CERT Relationship

- The ictQATAR vision recognizes that information security is critical to its success
- CERT/CC vision recognizes that information security in the Middle East is critical to global success
- The synthesis of these two visions produced the working relationship between the ictQATAR and the CERT/CC that is Q-CERT
- “Q-CERT will build cyber security capability and capacity in government and private sector organizations in **Qatar and the Gulf region**”

The Evolving Relationship

Current



ictQATAR

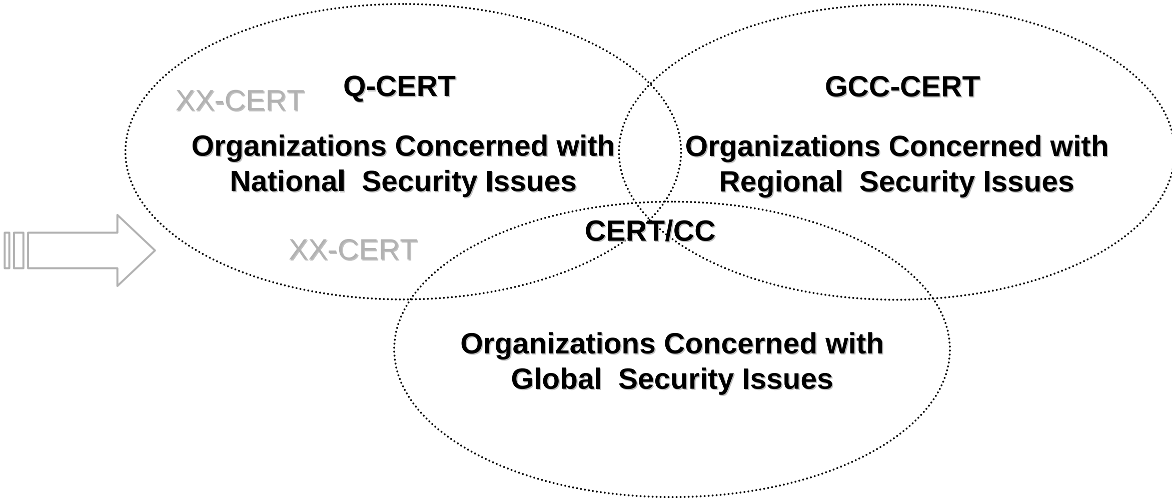
Carnegie Mellon University

Software Engineering Institute

CERT/CC

Q-CERT

Future



XX-CERT

Q-CERT

Organizations Concerned with National Security Issues

XX-CERT

GCC-CERT

Organizations Concerned with Regional Security Issues

CERT/CC

Organizations Concerned with Global Security Issues

Q-CERT

Current Operations

ict QATAR قطر

Q-CERT

- An asset with a national mission
- A Regional Resource

Q-CERT Vision

Q-CERT will be a world-class Center of Excellence in Information Security conducting national and regional programs in cyber threat and vulnerability reporting, incident response, and security improvement.

Q-CERT will be recognized in the nation and the region as:

- an objective, unbiased source of cyber-security information
- a champion promoting security standards, practices, products, and services that are most effective at mitigating cyber risks
- a trusted confidant and ally in coordinating responses to cyber-security incidents
- a leader in building cyber security awareness, understanding, capability, and capacity in both public and private sector organizations

Q-CERT Mission

Q-CERT will build cyber security capability and capacity in government and private sector organizations in Qatar and the Gulf region

- provide information and training to build the management and technical skills needed for organizations to effectively manage their cyber risks
- serve as a central, trusted partner in security incident reporting and analysis
- provide accurate and timely information on current and emerging cyber threats and vulnerabilities
- respond to significant threats and vulnerabilities in critical infrastructures by conducting and coordinating activities needed to resolve the threats
- promote and facilitate the adoption of standards, processes, methods, and tools that are most effective at mitigating the evolving risks

Q-CERT Constituents

- all Qatar domains (.qa)
- all users of the Internet in Qatar
- Cyber Forensic investigators in Qatar

Characteristics of Constituency

- Few / No product vendors / software developers
- Emerging IT capabilities
  - Broadband penetration
- IT Infrastructure jumping generations –
  - Rather than suffering through generations of maturation acquiring tested and matured systems
- Cultural bias / concerns
  - Implicit trust model
- Generational Gap
  - Speed of capability availability impacting acceptance and comfort with use
- Legal guidelines emerging
- Leadership position in Middle East

Areas of Work

- Critical Infrastructure Protection
- Watch, Warning, Investigation and Response
- Outreach and Training

Critical Infrastructure Protection

Critical Infrastructure Protection

- Assist key national resources in identifying and addressing information security vulnerabilities and threats
- Extend lessons learned from sector representatives to other members of that sector
- Develop and provide approaches for damage assessment and recovering operations from affected systems
- Identify areas of research appropriate for each sector

Critical Infrastructure Protection Strategy

- Initiate work with leaders in each sector – Strategic Partners
- Leverage experience to develop sector focus

Q-CERT Strategic Partner Services
- Identifying security needs -

- Strategic partner's mission/business goals?
- Infrastructure that support the goals?
- Strategic partner's security requirements?
- Policies, practices, technologies, and skills support requirements?
- Gaps and risks?

Q-CERT Strategic Partner Services

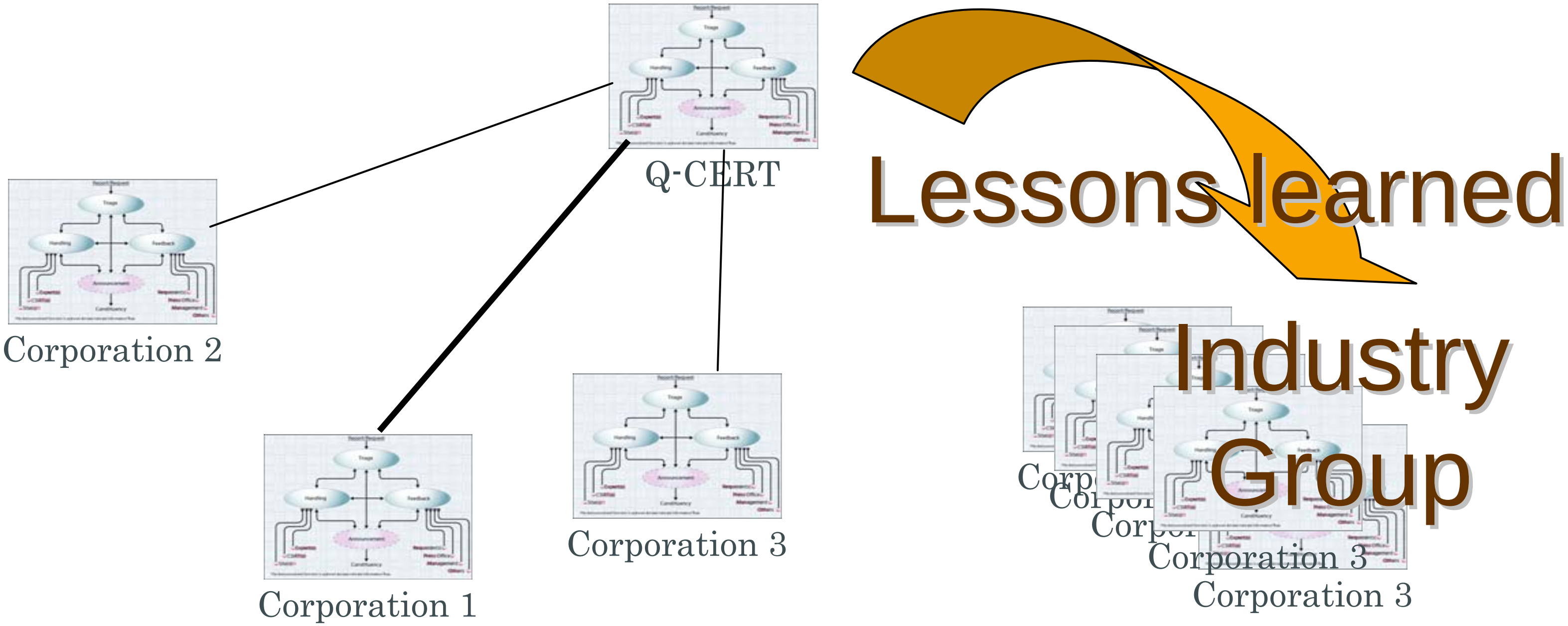
Implementing security enhancements

- Support planning for needed enhancements
- Support for policy, practice and technology enhancements
- Provide packaged courses and tailored training & mentoring
- Provide alerts on significant vulnerabilities and threats
- Provide incident response support

Q-CERT Strategic Partner Services - Meeting community needs -

- Provide structured methods to identify common needs
  - Surveys, focus groups, advisory boards
- Initiate special projects to meet common partner needs

Critical Infrastructure Protection Example



Q-CERT

Corporation 2

Corporation 1

Corporation 3

Lessons learned

Industry Group

Corp

Corpor

Corpor

Corporation 3

Corporation 3

Lessons Being Learned -

- Working with Strategic Partners
  - Set realistic expectations
  - Manage expectations over time
  - Capture lessons learned
  - Return real value
- Establishing Vertical Influence
  - Bringing disparate groups together
  - Removing competitive barriers
  - Work on common goals for the common good

Q-CERT

Watch, Warning, Investigation and Response

ict قطر QATAR

Watch, Warning, Investigation & Response

- Goals -
  - Assist in the creation of cyber-crime and privacy laws.
  - Establish agreements with law enforcement and other responders organizations.
  - Establish a national and regional center for threat, vulnerability, and security event data.
  - Establish and operate mechanisms for responding to cyber threats and vulnerabilities

Watch, Warning, Investigation & Response

- Monitoring
  - Watch native language web sites for activities related to cyber incidents
  - Watch English language web sites for information germane to constituency
  - Monitor internet traffic for patterns of interest
- Alerts
  - Developing target list of clients
  - Early warning to key constituents
  - Strategic Partners to get custom tailored alerts
  - Distillation of warnings and presentation in Arabic and English
- Incident Response
  - Based on reach-back capability
  - Primarily for high profile clients

Watch, Warning, Investigation & Response

- Computer Forensics
  - Assisting Law Enforcement in Qatar
    - Training in basic and advanced computer forensic techniques
    - Assistance in establishing forensic labs
    - Liaison with experts in the field
    - Building a community of expertise in Qatar

Q-CERT

Q-CERT Outreach and Training Plan

ict QATAR قطر

Outreach, Awareness and Training

Serve as a forum for national dialog on cyber security and create mechanisms for ongoing awareness and understanding of cyber security issues within public and private institutions and amongst the general public.

Outreach, Awareness and Training Strategies -

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

Q-CERT Curriculum in Information Security

- Creating a Computer Security Incident Response Team (CSIRT)
- Managing Computer Security Incident Response Teams
- Fundamentals of Incident Handling
- Advanced Incident Handling
- Information Security for Technical Staff
- Advanced Information Security for Technical Staff
- Computer Forensics for Technical Staff
- OCTAVE Training Workshop

Lessons Being Learned

- Training needs of constituents
  - How many workshops? What topics?
- How to handle logistics
  - Venues
  - Hours
  - Food
- Marketing
  - How to identify potential customers

What Have You Done for Qatar Today?

Current Activities

1. Outreach - articles, interviews, presentations, schools
2. Training – perpetual!
3. Critical Infrastructure Protection
4. Strategic Partners – needs assessments
5. Incident Reporting and Response
6. Regional Cooperation - facilitation

Going Forward

	July	August	September	October
workshops		Cyber-Forensics	CSIRT I CSIRT II	Advanced ISTS
conferences	National CSIRTs		Exec Briefing Korea TC	Brazil TC
forensics Project		National Lab Program		Training Academy Boot Camp
regional outreach	GCC-CERT charter meeting	GCC country visits	GCC-CERT Steering Comm.	GCC CSIRT training
		----→	---→	----→

Observations – the Good

- The need is acknowledged
- The core team is experienced
- The sponsor is committed long-term
- The relationship with CERT/CC is strong
- Our counterparts are motivated
- We are building on the accumulated experience of the CERT community

Observations – the Challenges

- There is a lot of work to do – the opportunities are endless
- Prioritizing the opportunities is critical
- Managing expectations is important – facilitation vs. operational roles
- Recruiting is “evergreen”
- The region is undergoing dramatic change – the skyline is just one manifestation

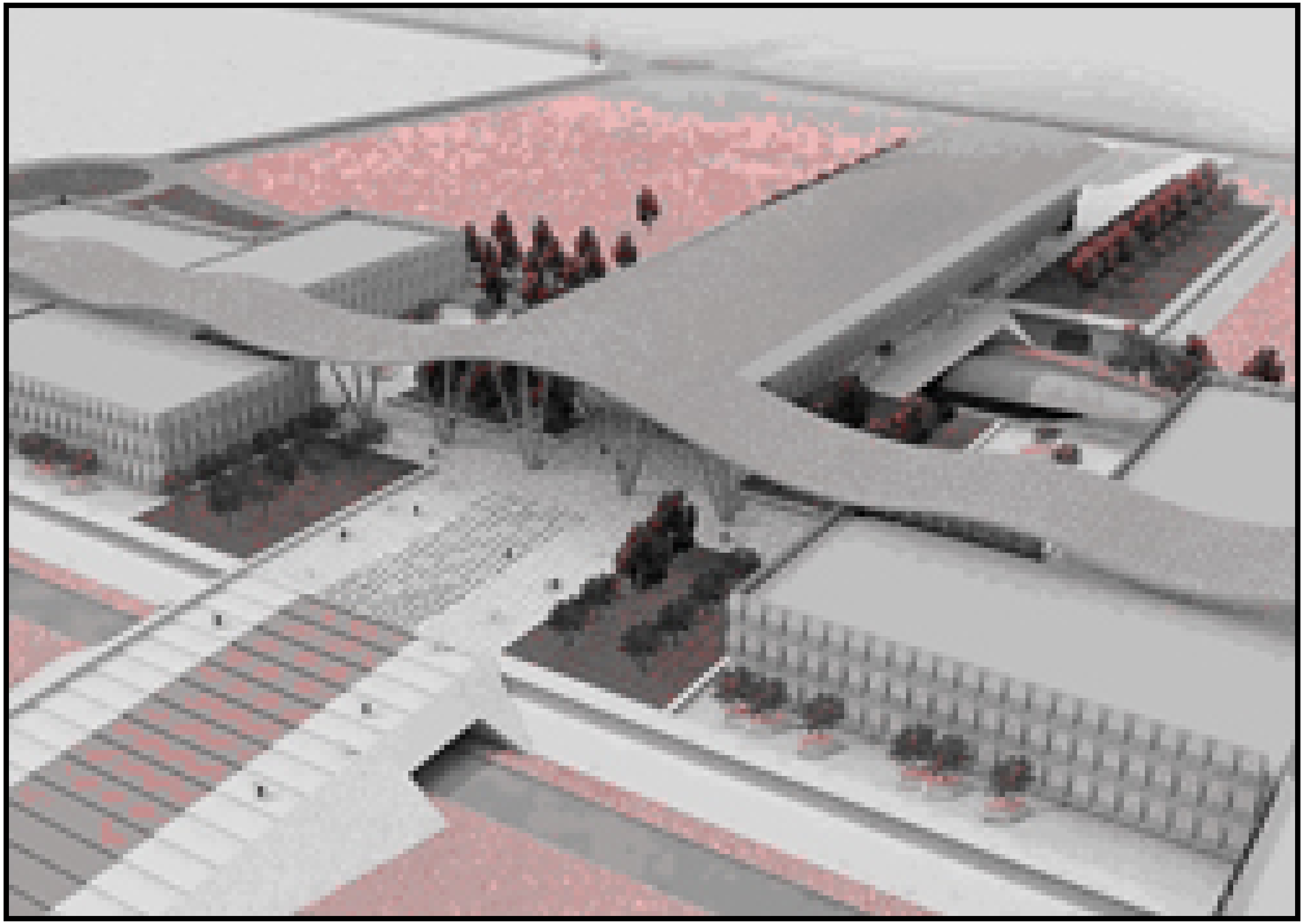
Doha – June ‘04

Doha – June ‘06

Lessons Learned

- Having sponsors and partners is good, but having several is complicated!
- Relationship building is vital, and ongoing
- People are reluctant to share ... incidents, data, vulnerabilities “d.n.e”
- Establishing proper facilities has proven to be more complicated than we envisioned - long term, temp, temp temp, t3 !

Our Future Home - STP



The End of Our Day
Questions?