Q-CERT

National Cyber Security Strategy - Qatar

Michael Lewis, Deputy Director

Coordinating a National Approach to Cybersecurity

ITU Pillars of Cybersecurity as a Reference Point

providing the collected “best practices” of the community

- Developing a National Cybersecurity Strategy
- Establishing National Government-Industry Collaboration
- Creating National Incident Management Capability
- Deterring Cybercrime
- Promoting a National Culture of Cybersecurity

Link Strategy to Vision

- The Emir of Qatar established the Supreme Council of Information & Communications Technology(ictQATAR) in 2004 as the primary ict organization in the country
- ictQATAR Vision: We *connect* people to the technologies that will *enrich* their lives, drive economic development and *inspire* confidence in our nation's future
- Attaining this vision requires secure, resilient information and communication technology

Q-CERT

- ictQATAR chose to build a national CERT as one of its first projects …
- … in partnership with Carnegie Mellon University
- A five-year start-up, with the intention of becoming a counterpart to the CERT/CC in the MENA region
- The national CERT is an important component of the overall national strategy for cybersecurity … but as we will see, not the only component!

Q-CERT Strategic Plan

- The core elements of the original project plan:
  - 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 (1)

- Create awareness at a national policy level about cybersecurity issues and the need for national action and international cooperation
- At Q-CERT, this is done through direct contact, briefings, workshops, and organizing specialized targeted events

Developing and Obtaining Agreement on a National Cybersecurity Strategy (2)

- Develop a national strategy to enhance cybersecurity to reduce the risks and effects of both cyber and physical disruptions
- This effort is shaped by the Q-CERT National Information Assurance Framework (NIAF) project, with a steering committee comprised of representatives from key Critical Sector Organizations

Developing and Obtaining Agreement on a National Cybersecurity Strategy (3)

- Participate in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents
- Q-CERT
  - Was the first national team in the region to join FIRST
  - was instrumental in founding the regional GCC-CERT
  - Hosted the WTDC 2006 meetings in Doha, which launched the Doha Agenda and authorized Question 22/1
  - Hosted the ITU regional event on Cybersecurity (Feb 2008)

Steps (1)

- Persuade national leaders … of the need for action … through policy-level discussions … ongoing
- Identify a lead person and institution … Q-CERT, acting on behalf of ictQATAR, long-term tbd
- Determine where the national CSIRT should be established … founded within ictQATAR
- Identify lead institutions for each aspect of the national strategy … NIAF project

Steps (2)

- Identify the appropriate experts and policymakers … and their roles … NIAF
- (Establish) cooperative arrangements for and amongst all participants … and mechanisms for cooperation amongst ... entities at a national level … NDAs, MoUs, NIAF
- Identify international expert counterparts … other national CERTs, MENOG, FIRST, ITU

Steps (3)

- Establish an integrated risk management process … the CIP group designed a hybrid assessment methodology
- Assess and periodically reassess the current state of cybersecurity efforts … quarterly, with comprehensive annual reviews
- Identify training requirements and how to achieve them … designed & implemented an aggressive professional development program

Map Capabilities onto the Framework

Dir	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).
IM	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.
OaT	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.

Use the Framework as a Way of Discussing Strategy

ITU Framework Area	Lead	Partner	Support	Q-CERT Activity
I. National Strategy		✓		ictQATAR National Information Security Framework project CERT Survivable Enterprise Management ITU and FIRST participation GCC-CERT development
II. Government-Industry Collaboration	✓	✓		Q-CERT CIP CERT Survivable Enterprise Management Sector working groups and direct work with CSOs
III. Deterring Cybercrime		✓	✓	Collaboration with ictQATAR Regulatory Authority CERT Forensic training for law enforcement
IV. Incident Management Capabilities	✓	✓		Q-CERT Incident Management CERT/CC direct participation in complex or wide-spread incidents CERT NetSA support for monitoring and analysis CERT Malware Database and advanced analysis support Q-CERT Cybersecurity Network Collaboration with ISP and law enforcement FIRST participation
V. Culture of Cybersecurity		✓		Q-CERT Outreach and Training Collaboration with ictQATAR/e-Education Collaboration with other organizations

Who’s in Charge?

As shown …a national CSIRT is a leading actor in a national cybersecurity initiative … but not the only one … identifying and tasking the appropriate leaders, and reinforcing their leadership, is important.

There should be a high-level national policy framework that defines the relevant policies, standards, and practices required to implement the national cybersecurity strategy.

Develop Metrics to Measure Progress

- Establish attainable objectives … and measure progress
- Some simple organizational measures:
  - Staff – number & skill level
  - Constituents – membership in CSN, number of organizational CSIRTS
  - Training – range and level of courses offered, number of people trained, organizations participating
  - Incidents reported, coordinated, analyzed
  - Technical data such as Honeynet probes and attacks
- Beware of false metrics … "number of incidents that would have happened …"
- And, as Karl noted, don't wait for the metrics!

Observations & Lessons Learned (1)

- The Framework helps identify key actors and their respective roles and responsibilities
- A national cybersecurity initiative needs a high-level champion
- Organizations want solutions, not problems!
- Provide guidance & support
- Establish good national & international partnerships

Observations & Lessons Learned (2)

- Know your constituents & keep channels open
- Build communities of common interest
- Conduct regular events (relevant, content-rich) to bring counterparts together
- Discussions can be as important as outcomes … but don't let discussions replace outcomes!
- Credibility is fundamentally important

Final Observations

- A national CERT is necessary but not sufficient to accomplish the greater goals of a national cybersecurity initiative
- It is important to identify the main actors and establish respective roles & responsibilities, coordination & communication
- As noted, most countries have not yet reached a high level of cybersecurity … aligning with the established best practices is useful
- And conducting the self-assessment can help identify what exists … and what remains to be done

www.qcert.org

Thank You