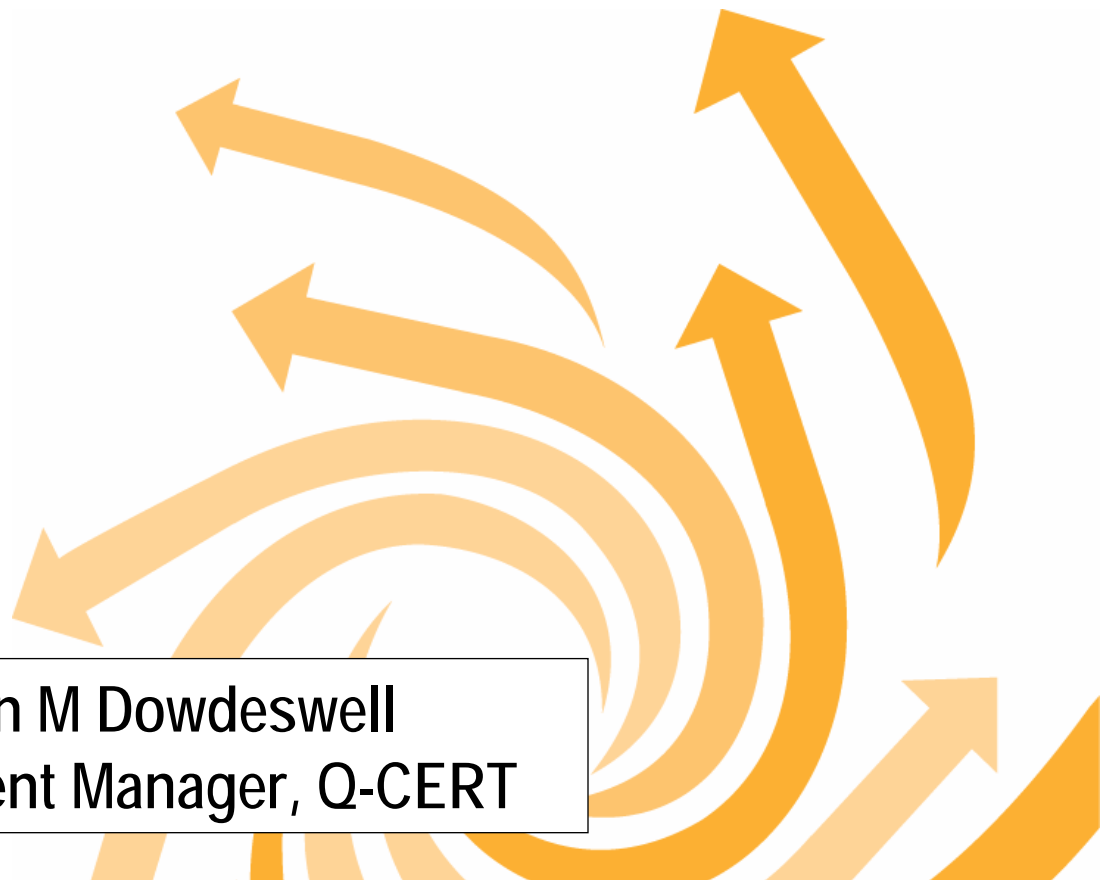


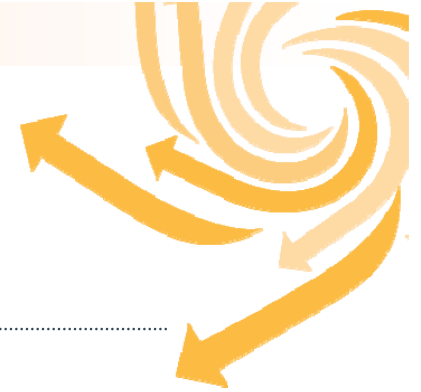


Presentation
to the ITU
on the
Q-CERT Incident
Management Team

Ian M Dowdeswell
Incident Manager, Q-CERT



Q-CERT Mission

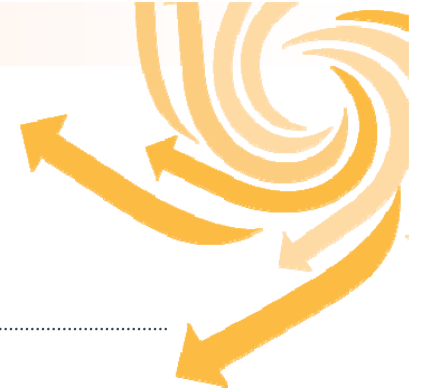


The Mission of Q-CERT is to be a world-class center of excellence providing expert assistance and support to improve information security in Qatar and the region.

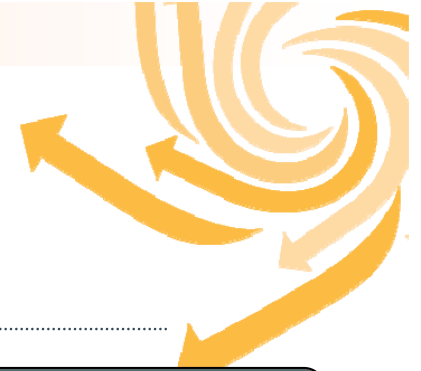


Q-CERT will:

- provide accurate and timely information about 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
- serve as a central, trusted partner in security incident reporting and analysis
- promote and facilitate the adoption of standards, processes, methods, and tools that are most effective at mitigating the evolving risks
- provide unbiased information and training to build the management and technical skills needed for organizations to effectively manage their cyber risk



Q-CERT Range of Activities

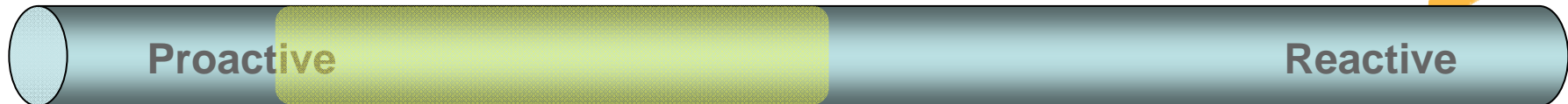
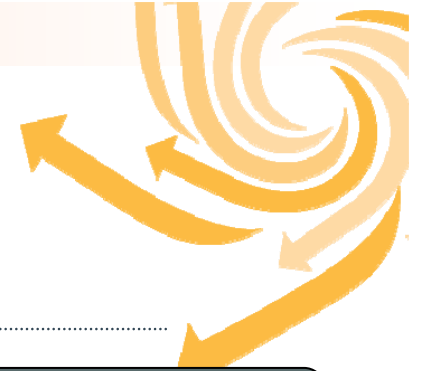


Outreach, Awareness, & Training

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



Q-CERT Range of Activities



Outreach, Awareness, & Training

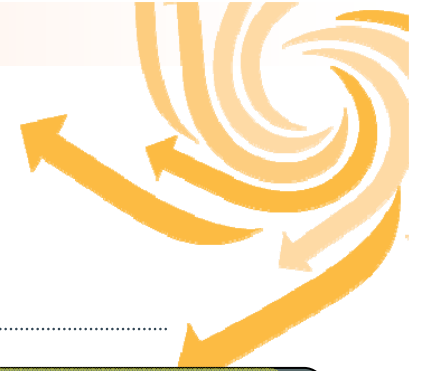
- Tailored workshops based on needs analysis
- Public workshops based on recognized needs
- Outreach to region

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



Outreach, Awareness, & Training

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

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

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.

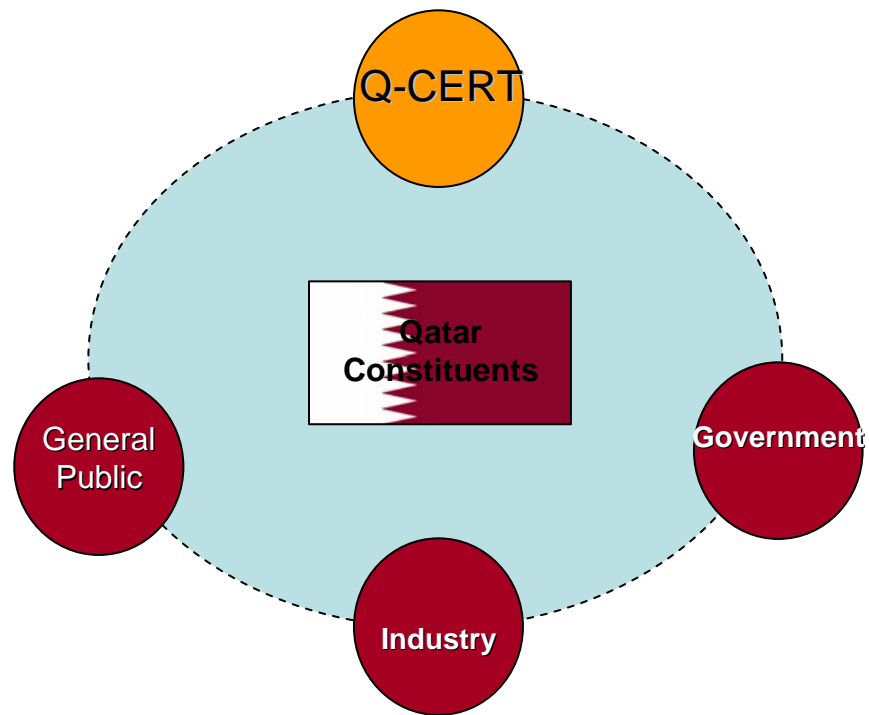


Q-CERT Potential Range of Activities

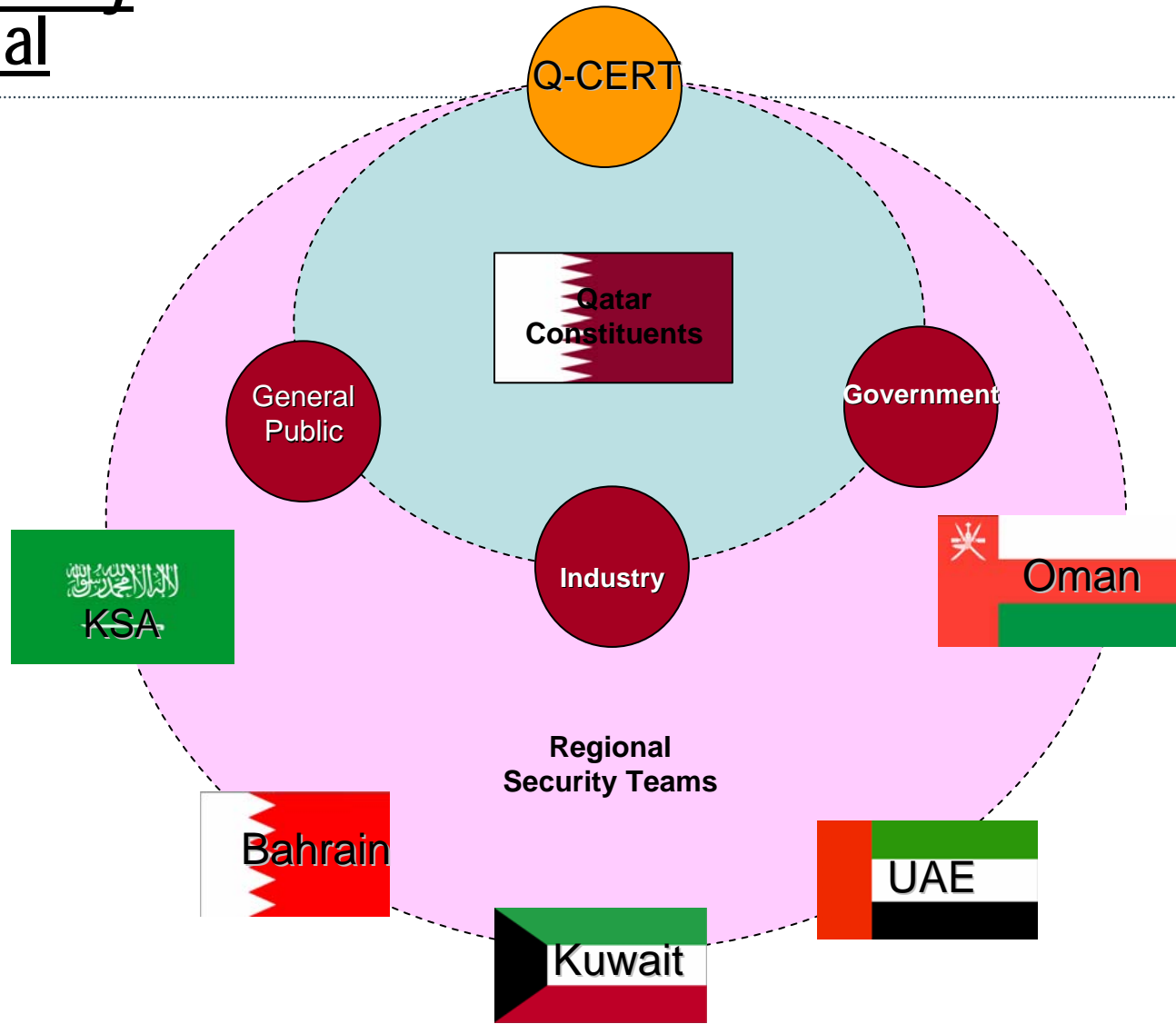
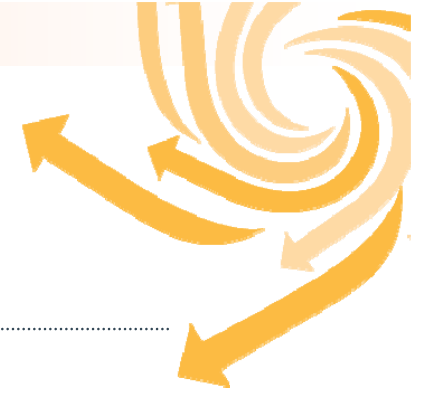
Reactive Services 	Proactive Services 	Security Quality Management Services 
<ul style="list-style-type: none"> + Alerts and Warnings + Incident Handling <ul style="list-style-type: none"> - Incident analysis - Incident response on site - Incident response support - Incident response coordination + Vulnerability Handling <ul style="list-style-type: none"> - Vulnerability analysis - Vulnerability response - Vulnerability response coordination + Artifact Handling <ul style="list-style-type: none"> - Artifact analysis - Artifact response - Artifact response coordination 	<ul style="list-style-type: none"> ○ Announcements ○ Technology Watch ○ Security Audit or Assessments ○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures ○ Development of Security Tools ○ Intrusion Detection Services ○ Security-Related Information Dissemination 	<ul style="list-style-type: none"> ✓ Risk Analysis ✓ Business Continuity & Disaster Recovery Planning ✓ Security Consulting ✓ Awareness Building ✓ Education/Training ✓ Product Evaluation or Certification



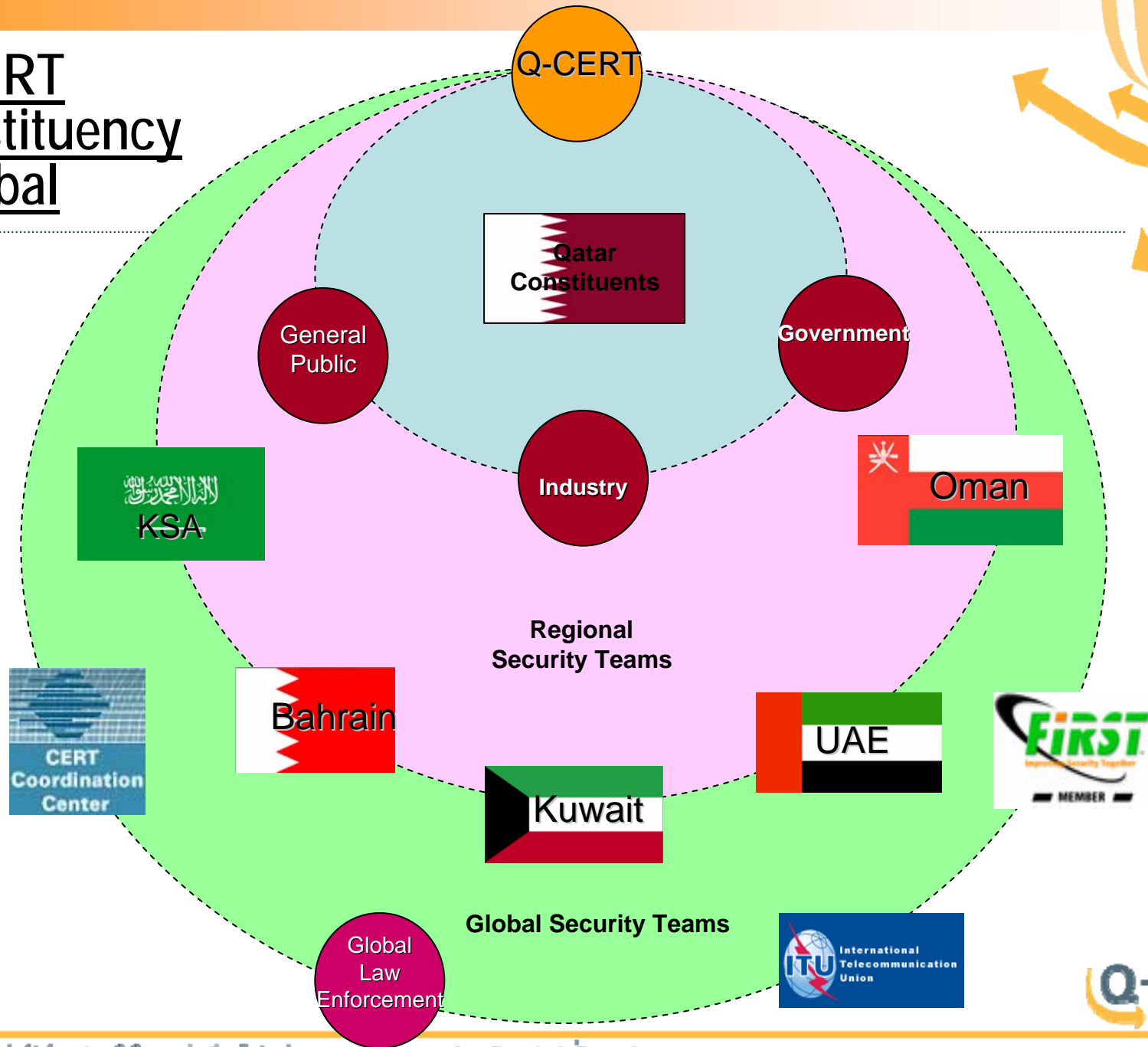
Q-CERT Constituency - National



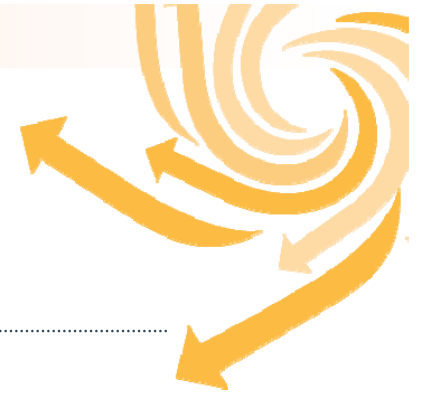
Q-CERT Constituency - Regional



Q-CERT Constituency - Global



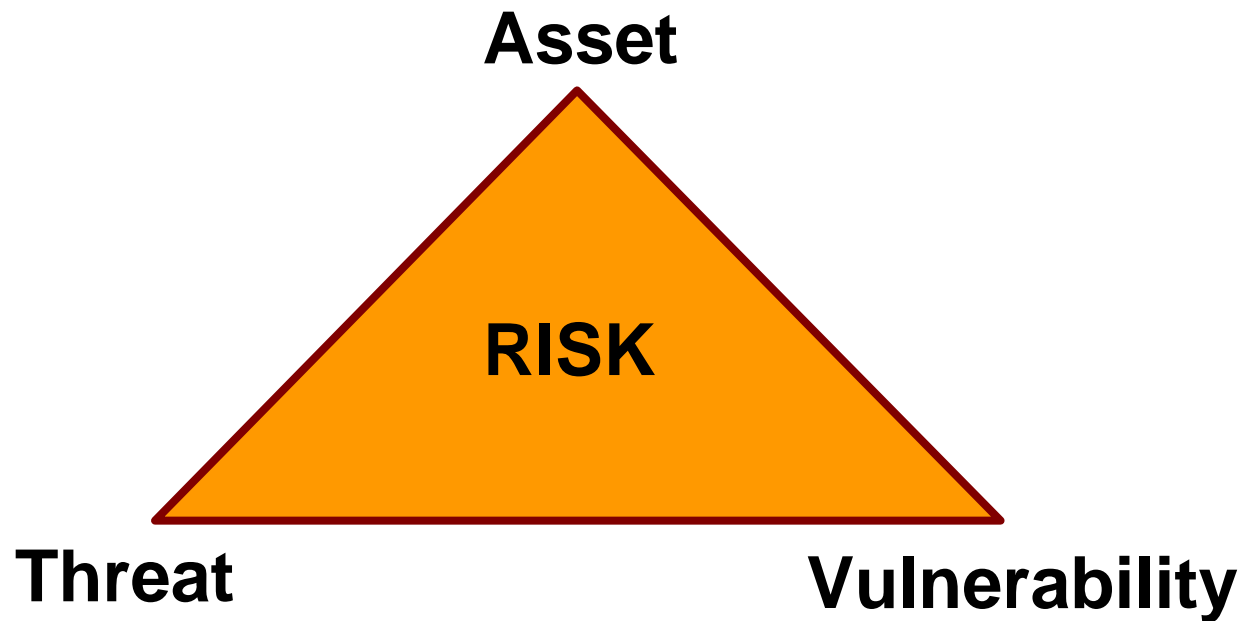
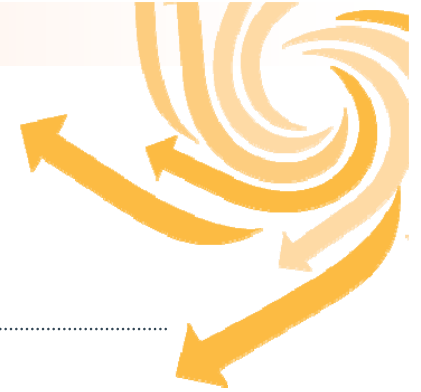
Incident Management Mission



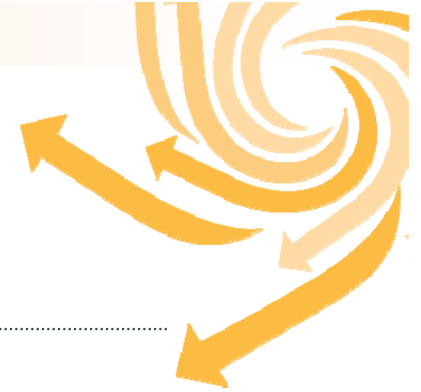
The mission of Q-CERT Incident Management is to enable our constituents to reduce the risk to their information (processed on computers and networks), through timely and effective provision of advice about threats and vulnerabilities and in response to incidents (where a compromise of information has occurred).



Components of Risk



Incident Management Activities

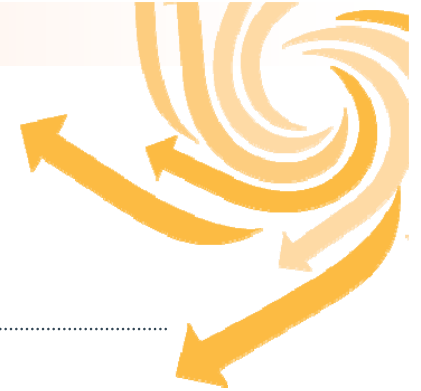


WATCH AND WARNING (WAW)

Mission. The mission of WAW is proactive to reduce the risk of compromise of constituent information by timely, accurate and relevant advance, guidance or best practice information to the constituent about vulnerabilities and threats to their information and networks.



WATCH AND WARNING (WAW) ACTIVITIES



Vulnerabilities

Role – identifies critical vulnerabilities relevant to Qatar and Region and disseminates to CSOs (primary) and citizens (secondary)

Generates vulnerability reports from all available existing vulnerability information.

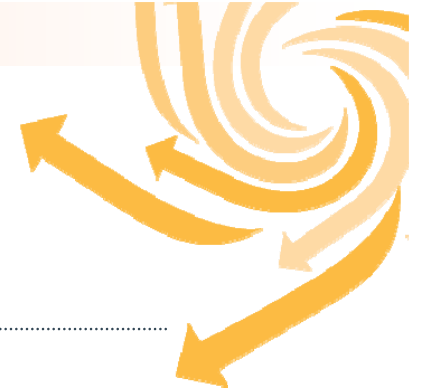
Scours websites for best practice including Middle East North Africa (MENA) sites.

Arabic capability.

Generates vulnerability reports primarily by email but also via e.g. SMS/website to mailing lists for focused output to constituents



WATCH AND WARNING (WAW) ACTIVITIES



Threats

Role – identifies ‘serious’ generic and specific threats to Qatar CSO and Region and informs selected recipients.

Looks at open-source threat information

Scours websites / hacker-sites / chatrooms

Links to SSB

Arabic capability

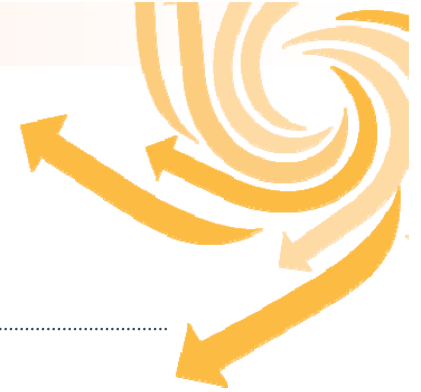
Generates threat reports to tailored community.

Runs honeynet / analyses data

Disseminates reports/briefings



WATCH AND WARNING (WAW) ACTIVITIES



Netflow analysis

Role – analyses packet traffic across national gateways to determine specific threats to nation and informs selected recipients

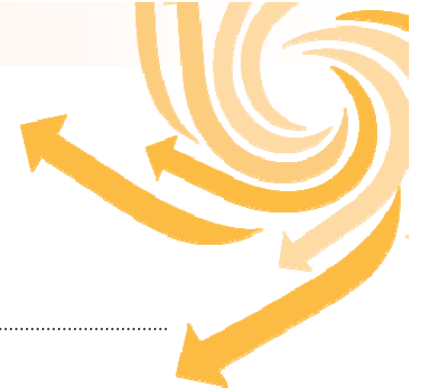
Analyses IDS data

Analyses Net SA data

Disseminates reports/briefings to selected recipients



Incident Management Activities

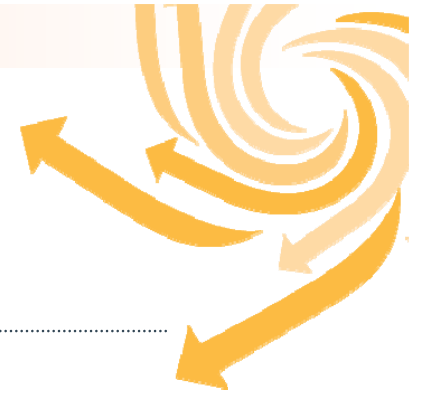


INCIDENT RESPONSE AND INVESTIGATIONS (IRI)

Mission. The mission of IRI is a reactive response to reduce the risk of further compromise of constituent information by responding promptly to an incident and providing timely, accurate and relevant advance, guidance or best practice information to the constituent and to follow up incidents through investigation, analysis and reporting.



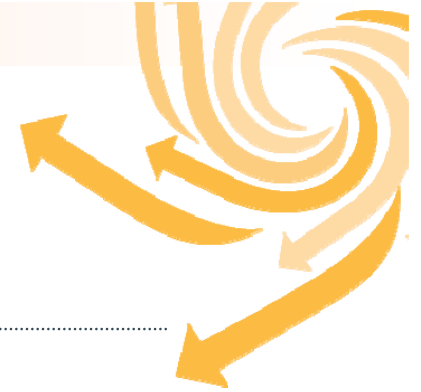
INCIDENT RESPONSE AND INVESTIGATIONS (IRI)



- Role – to provide an incident response capability to enable Qatari and Regional CSOs to reduce their risk following a compromise.
- Provides 24 x 7 cover for immediate incident response
- Triage
- Hotline / website / email etc.
- Site visits for investigation
- Artifact collection
- Artifact analysis / forensics
- Constituent / law enforcement / global liaison
- Investigation including technical / procedural and forensic
- Briefings and report writing



Incident Management Activities



Incident and Crisis management co-ordination

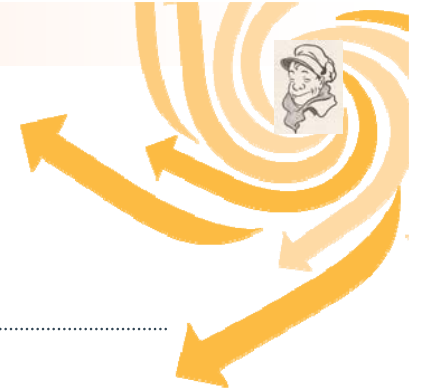
- co-ordination of localized incidents and major crises across sectors and between regional CERTs.



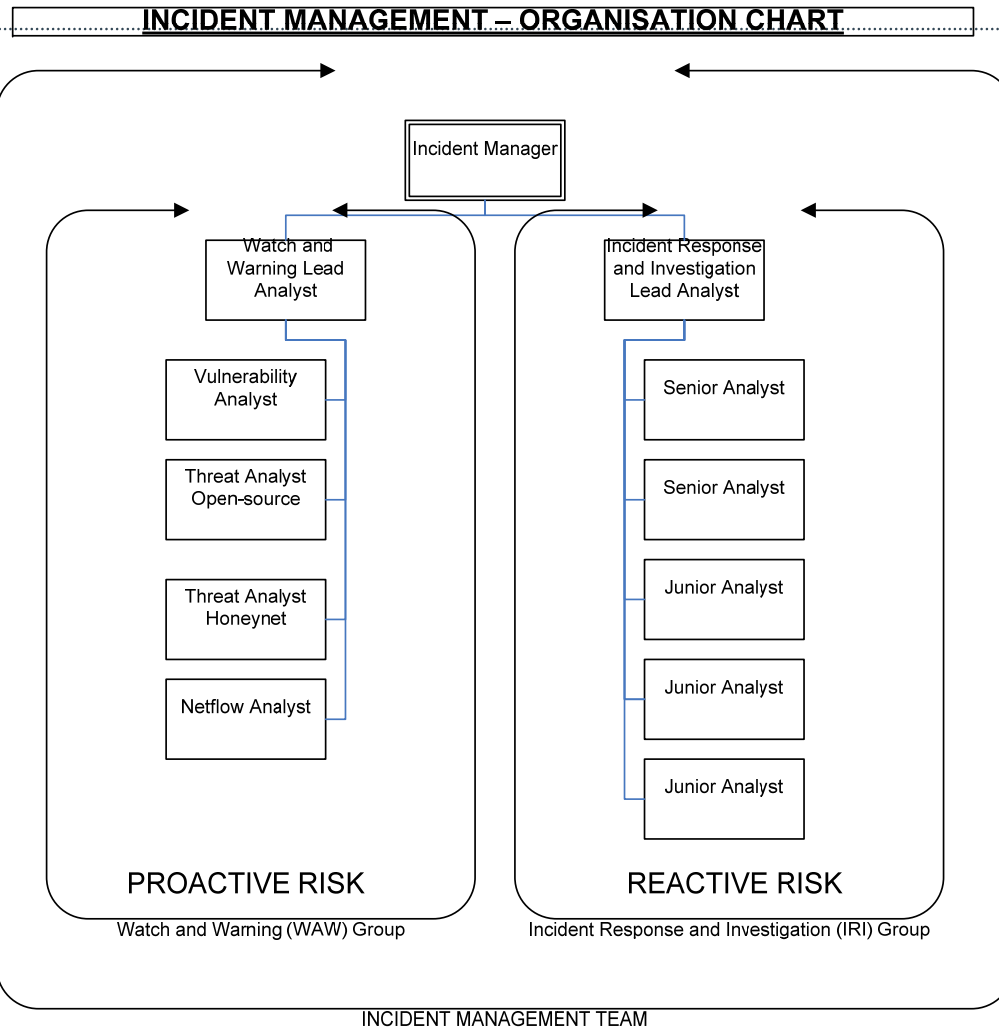
Specialist 'Lab Services'

- ▶ Vulnerability Assessment
- ▶ Malware Analysis
- ▶ Open Source Threat Analysis
- ▶ Vulnerability Analysis
- ▶ Computer Forensics
- ▶ Honeypot Analysis
- ▶ Network Flow Analysis

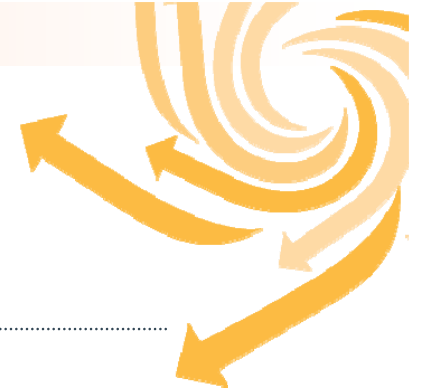




IM Organisation



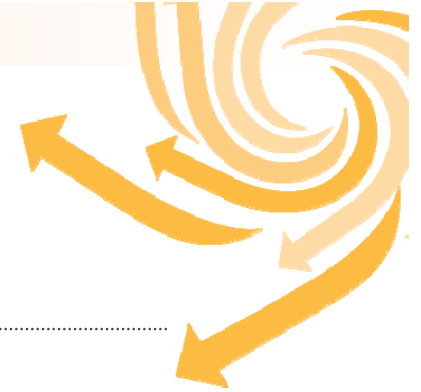
Cyber Security Network



The Cyber Security Network has been created to bring together the Critical Sector Organisations in Qatar and the region, to better understand their information security requirements and to enable Q-CERT to focus its output to meet them.



Cyber Security Network



Q-CERT can help CSO's to reduce the risk to their critical information.

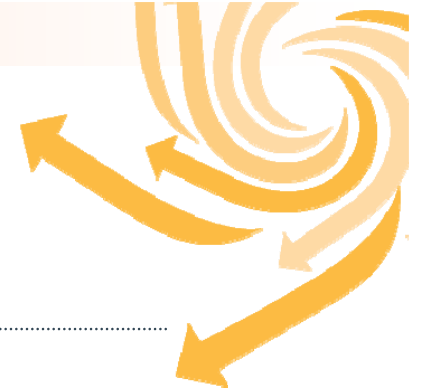
Q-CERT works with other security teams world-wide to maintain awareness of global trends and respond to international threats.

Q-CERT provides a range of services.

Q-CERT can help organizations improve their internal 'first responder' practices.



Cyber Security Network



Joining the program:

Non-Disclosure Agreement (NDA)

Establish formal points of contact.

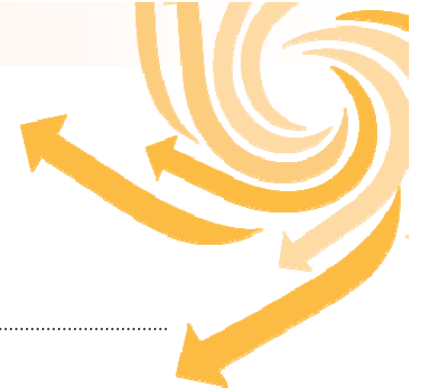
Orientation briefings

Ongoing training

Long-term Critical Infrastructure Protection (CIP) program



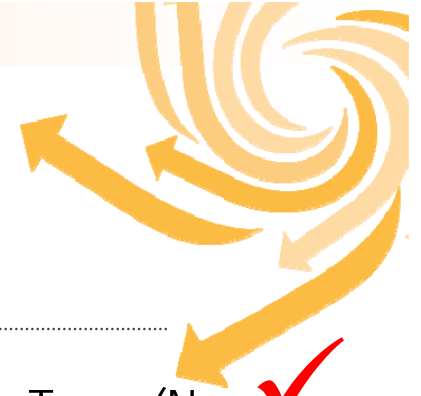
ITU - Incident Management Capabilities



- ▶ Develop a national cyberspace security response system to prevent, predict, detect, respond to, and recover from cyber incidents.
 - Watch, Warning, Response & Recovery ✓
- ▶ Develop a national cyberspace incident management program in coordination with the intelligence and law enforcement communities. ✓
- ▶ Participate in watch, warning, and incident response information sharing mechanisms. ✓



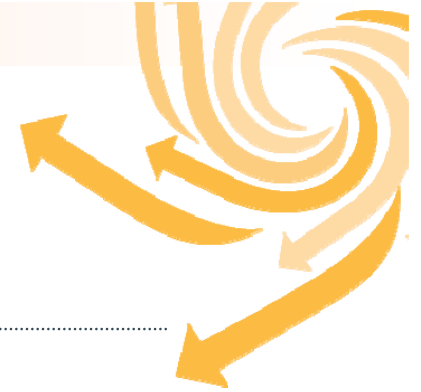
ITU – National Computer Security Incident Response Team Capabilities



- ▶ Identify or Establish a National Computer Security Incident Response Team (N-CSIRT) ✓
- ▶ Ensure N-CSIRT Coordination with Industry ✓
- ▶ Establish Points of Contact with N-CSIRT ✓
- ▶ Participate in International Cooperative and Information Sharing Activities ✓
- ▶ Develop N-CSIRT Tools and Procedures ✓
- ▶ Develop N-CSIRT Capability to Respond and Recover ✓
- ▶ Promote Responsible Disclosure Practices ✓
- ▶ Promoting a National Culture of Cybersecurity ✓



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

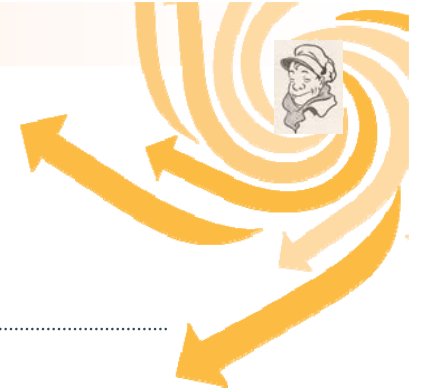


Incident Manager –

Ian M Dowdeswell

imd@qcert.org





Questions?

Questions?

