

Q-CERT works with government and industry to develop and lead a multi-pronged approach to managing cyber-security risks.



SECURITY FOREMOST

Q-CERT was established as Qatar's premier national and regional organisation to conduct and coordinate comprehensive cyber-security activities. Q-CERT Director, Dr Rashid Al Ali talks expansively about the various functions of Q-CERT.

What was the inspiration behind the formation of Q-CERT? What are its broad functions?

Qatar is committed to have a safe Internet experience and ensuring that every business transaction be secure. The clear lack of any such formal initiatives in the country and the region was seen as a barrier and risk to a robust information-based society envisaged by the government of Qatar. To

ensure that these risks were dealt with from the start, Q-CERT was set up.

Q-CERT builds information security capability and capacity in the public and private sector in Qatar and the region by working across the following areas:

Critical Infrastructure Protection (CIP): Critical Infrastructures are those key industries, institutions, and distribution capabilities that are essential to the defence and economic security of the nation and the smooth function of government and society as a whole. The ultimate goal is to protect Qatar's critical infrastructure by reducing the risk of interruption, modification or disclosure of existing as well as

emerging technology based systems.

Incident Management: Q-CERT's Incident Management function enables constituents to reduce their information risk through timely and effective provision of advice about threats and vulnerabilities. It also provides experienced and professional Incident Response.

This is achieved through: Threat and Vulnerability Assessment, Threat & Vulnerability Information Dissemination, Incident Analysis and Response, Incident Investigation, Incident and Crisis Management Coordination.

Outreach and Training: Q-CERT's Outreach and Training program is de-

signed to provide progressive levels of information security training to our constituencies -- from seasoned IT professionals to the general public. The core areas of this program focus on technical security issues, executive decision making, open discussion forums, and general security awareness.

Analysis Labs:

Q-CERT has focused on establishing a number of core competencies that provide the tools to better understand and analyse constituents' security posture as well as the state of the practice within Qatar and the region.

Is Q-CERT meant only to protect the critical infrastructure of the nation or will it serve the nation as a whole?

Q-CERT is positioned and is specifically designed to protect both the Critical Infrastructure as well as the nation as a whole. Both are important to Qatar as it works to achieve its broader social, political and economic goals.

What about the component that covers security at home/home users?

Through our website, we provide security alerts and guidance on best practices for home users. We provide Information Security advice directly to students, teachers and parents through our schools outreach initiative. In addition, we hold the bi-monthly Qatar Information Security Forum (QISF) which is open to the public and

covers specific Information Security topics the attendees want to discuss. Presentations at QISF are provided by world renowned experts in the field of Information Security.

Which are the other agencies that work in conjunction with Q-CERT?

We work with a number of other organisations and agencies both locally as well as internationally. Typically this ranges from local entities such as, law enforcement, sector regulators, to government and private entities. Internationally, we work with CERTs and Critical Infrastructure Protection organisations around the world.

What are the achievements of Q-CERT so far?

Q-CERT has engaged with various partners within the country and the region to help improve Qatar's information security practices.

Q-CERT has identified the need for Qatar's Critical Infrastructure to be protected, and has begun engagement with various industries such as, banking & finance, oil & gas, communications, healthcare and government. Q-CERT is taking a risk-based approach to help secure the country's Critical Infrastructure by providing tools, methodologies, and guidance on risk assessment, analysis, and mitigation.

Q-CERT has also begun providing computer security Incident Management services to Qatar. Q-CERT has

already had several successful engagements, assisting companies with analysis, recovery, and remediation of security incidents. Q-CERT has assisted such organisations across industries from government, education, to banking.

Q-CERT has engaged in many different Outreach & Training programs, offering courses to the Qatar business, government, and educational communities to increase information security knowledge. Q-CERT has offered courses on technical security, incident handling, and security awareness.

What is the role of Carnegie Mellon University in the formation of Q-CERT?

Carnegie Mellon is a global research university, recognised for its world-class technology programs, collaboration across disciplines and innovative leadership in education.

It is the home of the founding CERT organisation, the CERT Coordination Center (CERT/CC) which is part of the world renowned Software Engineering Institute (SEI). By leveraging the experience and wealth of skills from within the SEI, Q-CERT has a springboard to launch its activities knowing that it has the support and assistance to achieve success.

What is the impact of being accepted into the FIRST community? What was the FIRST Technical

“Q-CERT has identified the need for Qatar’s Critical Infrastructure to be protected, and has begun engagement with various industries such as, banking & finance, oil & gas, communications, healthcare and government. ”

Colloquium about?

As a member of FIRST, Q-CERT is able to connect with the global computer information security and incident response community with its wealth of expertise, knowledge and experience. This will enhance our knowledge of vulnerability and threat information, leading to a greater understanding of risks facing the Qatar IT community. FIRST will also provide a valuable additional source of expertise to assist with our response to any incidents that might occur.

The FIRST Technical Colloquium (TC), the inaugural Middle East FIRST event, consisted of a week of conferences, workshops and panel sessions covering cyber forensics, fraud, identity theft, phishing, organisational risk assessment, network flow analysis, as well as other issues. The event was well received by all who attended and set a benchmark for similar future events.

What are the areas of vulnerabilities in Qatar that one should be aware of? How has the Incident Response been so far?

Qatar is subject to the same threats and vulnerabilities as the rest of the Internet community. Currently, the single greatest threat is from malicious software and robotic networks (botnets) with their links to fraud and identity theft. We are taking proactive steps to detect and mitigate these threats. At present, our aim is to make

the residential and business users aware of the problem and to take the best possible measures to protect them from compromise. We do this through available tools such as anti-virus software, firewalls and anti-spyware applications. The use of well-established procedures, such as good password management, awareness of the risks and using common sense when reading emails and accessing untrusted websites is also crucial.

How would you assess the security levels in the country in these categories: a. home users, b. small and medium enterprises, c. governmental, d. large corporations.

Home users: It's truly hard to assess the security of this community because of the lack of awareness amongst home users. Most end-users are only aware of a problem if their anti-virus tells them, and since many of the modern pieces of malware out there can disable anti-virus, the end-user is unaware of the infection. Studies by the CERT/CC, and others (CIS/FBI, AusCERT) show that the vast majority of botnets are run from home users with broadband Internet access, so it is a significant problem. By carrying out surveys, setting up HoneyPots and working with the local ISP, we hope to assess the security levels of home users.

Small & medium organisations: This group typically faces the largest (in total and percentage)

dollar value loss as a result of security incidents due to the lack of awareness and resources. This is also the group most likely to use managed/hosted services, sometimes making them unaware that a breach has occurred. By carrying out annual nationwide surveys, we are planning to obtain information on security maturity in the organisations as an initial baseline. We will revisit this on an annual basis to measure improvement over time.

Government: Government entities are consistently under scrutiny by external audits undertaken to assess their effectiveness. By working directly with some of these partners, we hope to obtain a good picture of security within the government sector. Additionally, we work closely with ictQATAR's government initiatives to ensure that future IT platforms are built and operated securely from the start, meeting defined standards and best practice.

Large enterprises: These typically have the best security because they have the resources to implement proper security policies, controls, and training. They are also the group to meet international standards and regulatory compliance. However, they often face the largest loss for single incidents. Through focus groups and direct interaction, we are aiming to obtain a better picture of security maturity in Qatar's largest enterprises ■

“Currently, the single greatest threat is from malicious software and robotic networks (botnets) with their links to fraud and identity theft. We are taking proactive steps to detect and mitigate these threats.”