Message from the Assistant Undersecretary of Cyber Security Sector

Today, our government, our industry, and our entire population, communicate, and socialize in a cyber-environment that relies on software-reliant IT architectures, applications, and services.

Gone are the days when the network was just a support infrastructure to a few basic organizational functions. Today and in the future, this cyber environment is foundational to and connected with almost everything we do.

However, as we have come to depend on this cyber world more, we face the risks that arise from this dependence. The size and complexity of this world mean possible exposure to disruptive, damaging events. These events stem from not only software quality issues, emergent behavior, and unforeseen dependencies, but also cyber-attacks by hackers, insiders and criminals.

The borders between the virtual and real worlds are dissolving, as new technologies, services and business models push existing concepts and regulation to their limits. The organizational structures and physical barriers that ensured security in the past are now largely obsolete, and in some cases, have been breached by cyber threats that are continually evolving. Taking positive, concrete steps to manage these challenges requires that we acknowledge the risks and costs of not addressing the challenges. It requires increased cooperation between all actors at all levels. Whilst cooperation will not happen overnight, Q-CERT will continue its mission to bring communities together and to encourage information exchange that is based on concrete goals. This will lay the foundation for a more effective collaboration model in the years to come.

Qatar aims to fully promote information and communication technology to become one of the most successful knowledge-based societies in the world. It is part of ictQATAR’s mission to bring Qatar in step with the best computing practices in the world, and this helps realize our goal.

Thus, it was with this foresight that the Ministry of Information and Communications Technology conceptualized setting up a dedicated body, the Cyber Security Program, to proactively and reactively address and respond to risks that may arise with technology use, which is in its 7th year of success.

Q-CERT was formed to seize and catalyze change, specifically to accelerate the widespread availability and adoption of effective cyber security measures, practice and policy.

Q-CERT’s goal is to identify, validate, promote and sustain the adoption of cyber security best practice-by people, with technology and through policy – to create a world in which best practice becomes the common practice.

The efforts of Q-CERT in the year 2014 is summarized in this annual activity report.

Sincerely

Eng. Khalid N. Sadiq Al Hashmi

Assistant Undersecretary of Cyber Security Sector

Ministry of Information & Communication Technology
Table of Content

1- Introduction
2- Cyber Security Intelligence
3- Cyber Security Resiliency
4- Public Key Infrastructure & Licensing and Identity
5- Cyber Security Training & Awareness
6- Cyber Security Risk Management
7- Cyber Security Crisis Management
8- Cyber Security Information Assurance
9- Cyber Security Policy & Standards
10- Memberships
Introduction

A digital device and a network connection are all it takes for anyone across the globe to tap into the vast world of loosely connected networks that we call the Internet. It gives organizations and individuals, no matter their national or geographic boundaries, the ultimate access to all the information and data they need. However, a door swings both ways and this access doesn’t come without risk. The main risk of having a presence in the digital world is that valuable information could be lost, stolen, changed or misused. System intruders have the ability to tamper with any type of information without touching a piece of paper or even being in the same country of the organization or the individual they are targeting. They can also create new electronic files, run their own programs, and hide any traces of their unauthorized activities. The traditional threats from intruders have been rapidly changing to include more malicious players such as hackers, organized criminal networks and industrial and foreign government espionage that includes cyber warfare to name a few. These risks and threats raised the need for immediate development of countermeasures and the concept of Cyber Security.

Recognized as a trusted, non-profit organization dedicated to improve the security and resilience of computer systems and networks in Qatar, Qatar Computer Emergency Response Team (Q-CERT) was established in 2005 as a national asset in the field of cyber security. Since its establishment, the Cyber Security Division evolved dramatically from a department coordinating response to internet security incidents to a complete division working on projects that take a proactive approach to secure systems.

While keeping Q-CERT as the preliminary identity, the division evolved to become the Cyber Security Team, which covers a wider spectrum of information security areas signified in critical infrastructure information protection including governance, risk and crisis management amongst other services and functions.

The team was established to address the cyber security needs and requirements in Qatar and provide the proper protection mechanism to minimize the associated risks. It also continues to understand and address the nation's information security needs through a number of reactive and proactive services and instills digital confidence in all constituencies in the country.

The Cyber Security Team gives every effort to bring unique solutions to cyber security challenges through constant partnership with the governmental, industrial, financial, health and energy sectors to develop advanced methods and technologies for systems counter large-scale, sophisticated cyber threats.

The Cyber Security Annual Report for 2014 is the first edition and is available to the public. Annually, the report will be published to showcase the accomplishments of Q-CERT during the year and summarizes 12 months of dedication and hard work and sets the Cyber Security Team's plans for the year ahead. The aim behind publicly publishing this report is to inform organizations in Qatar on the local cyber security scene and help entities plan for the upcoming year cyber-security wise, yet the team honors its confidentiality promise in this report and all the editions to follow.
The Report Summary:

- Malicious software is the highest cause of incidents in Qatar
- Informative Incidents are the highest number of incidents solved in Qatar
- Highly Sever Incidents are the lowest number of incidents solved in Qatar
- Spam is the highest threat detected in Qatar
- Conficker malicious software still propagate in Qatar and dominate the number of detection
- Cyber security technical resiliency assessments indicate a need to focus on Web Application Security
- The signing of the first Certification Service Provider License, developed by the Cyber Security Team, by H.E. Dr. Hessa Al-Jaber, the Minister of Information and Communications Technology
- Training over 100 information technology and security professionals in Qatar with 75% being Qatari nationals
- The development of Information Security Risk Management Framework
- Conducting thirty on-site information security assessments to critical infrastructure information organizations
- Conducting a successful second cyber drill, Star-2 with the participation of over 400 information technology and security professionals.
1. Incident Handling and Digital Forensics

In the cyber world, even with the most sophisticated countermeasures in place, there are no guarantees that incidents will not happen. Attackers seize opportunities, or in other words 'vulnerabilities', and take advantage of them to conduct their malicious activities. Incident response and digital forensics are two reactive measures that help quarantine damages, restore operations and capture criminals.

Vulnerabilities exist behind every incident and threats exploit them by targeting one or more elements of the three business operation pillars: people, process and technology.

Incidents can be categorized in many ways. This report exhibits incidents detected or reported to the Cyber Security Team according to the following categories: threat types, severity level, sector specific and distribution throughout the year.

The total number of incidents triaged by the team in 2014 has increased by 16% since 2013. This increase is governed by many factors one of which is the increasing number of threats. Other factors could be attributed to a better knowledge of the Cyber Security Team’s work in this area and a higher level of information security maturity by professionals in other organizations; hence, more incidents are reported.

Malicious software, phishing, spam, fraud and intrusion are some examples of cyber threats that were encountered during 2014 (see Figure 1). The category with the highest number of incidents was malware infection which caused 56% of the total number of incidents. This is no different to the international threat landscape which also detects malware to be the highest threat in 2014.1

This high number of malware infection falls back to the ease of its development and propagation. New tools and exploitation kits provided by the underground community have made malware development accessible to everyone regardless of the level of acquired knowledge. The high propagation rate of malware reverts to the existence of high performance technology infrastructure and the low detection levels of anti-malware software.

The incidents associated with malware were not limited to organizations, but also extended to home networks. A wide range of operating systems was used on the infected systems and; hence, no specific system is completely immune.

---

1 This information is based on the Cyber Security Team’s findings and a number of information security reports for 2014 such as SIR2014, 3Q 2014 TrendMicro and Security Threat Report 2014 SOPHOS.
The second category with the highest number of incidents in Qatar was phishing which caused 9% of the total number of incidents. Since 2013, the number of phishing attacks had increased by 44%.

Phishing utilizes the deceptive techniques of social engineering and targets a wide range of audience from organizations to home users. The most crucial attacks have been targeting critical infrastructures in Qatar. The reason behind the increase in phishing rates can be that the attack is used as a preliminary tool to possess credentials that aid in launching more sophisticated attacks. The ripple effect of phishing is very high and fast and it can easily target a large number of victims concurrently. Phishing rates could be high, as well, because of the attacks nature of exploiting the chain of trust. In other words, if the attacker exploits an account of one person in an organization and starts sending phishing messages on behalf of that person to other users in the same organization, they are most likely to fall for the trap. Those reasons amongst others underline the need to increase awareness efforts in this regard to educate users and citizens to be capable of detecting fraud.

The largest percentage of incidents was informative (see Figure 2). This category resembles incidents that were detected or reported to Q-CERT for verification and required no further technical intervention.
as most of those were spam or malware infection detections. There were no severe\textsuperscript{2} incidents triaged by the Cyber Security Team in 2014.

![Pie chart showing incident severity levels in 2014]

\textbf{Figure 2:} The level of severity for incidents in 2014

Incidents also are not limited to certain entities as threats can extend and harm all sectors. Many critical infrastructure sectors in Qatar had encountered incidents in 2014. It is noted that the energy sector faced the most incidents with 18\%, to be followed by the banking and finance sector with 16\%, government with 14\% and the education sector with 12\% (see Figure 3).

Since 2013, the number of incidents has increased in some sectors while it decreased in others. However these variations in numbers are not an indicator that some sectors have become more secure than others. Yet those numbers are pointers to important areas of research and analysis.

\textsuperscript{2} Incident severity levels are classified by Q-CERT as: Severe, high, medium and low. A complete incident severity policy is found at www.qcert.org.
While there was no pattern detected yet to govern the distribution of incidents throughout the year, the number of incidents increased towards the second half of 2014 (see Figure 4). A possible reason could be that most popular vacations, such as summer and winter, are taken place in the second half of the year and the dates of some of the major triaged incidents throughout the year supports this assumption.
The Cyber Security Team performs incident response and digital forensics all year long through:

Q-CERT Incident 24/7 Hotline: +974 4493 3408

Q-CERT Incident reporting form on www.qcert.org
2. Cyber Security Intelligence

Cyber threats and security attacks are growing in numbers and becoming stronger and more aggressive all around the globe. Qatar, being a rising state in the global scene, is no exception to those threats. In order to reduce and prevent them, proper researches and analysis must be conducted.

To stay vigilant against possible cyber threats, the Cyber Security Team focuses on monitoring and studying cyber threat landscape in addition to developing security analysis tools that help in threat detection.

A. Threat Monitoring System
The threat monitoring system (TMS) was internally developed by the Cyber Security Team in 2011. The system collects threat information\(^3\) from worldwide sources, aggregates and parses those feeds and then analyzes what threats are relevant to the nation. Hence, to help proactively counterpart those threats, alerts are sent to government and critical infrastructure organization from threats that may possibly target their networks. The collection of data happens through agreements with international organizations, vendors and international government organizations. The threat monitoring system is capable of processing tens of millions of records.

During the year 2014, over 14 million records of threat information was processed. The number of threats detected and discovered in Qatar during the year reached 2 million infections covering home and corporate networks. In response to these numbers, over 30,000 possible threat alerts have been sent to notify Q-CERT’s Incident Handling Team to start verification, investigation and implement countermeasures.

This is different from the public and the sector specific or restricted alerts discussing large-scale threats. In that regard, the Cyber Security Team has issued eight alerts (7 Informative and 1 Critical) through the Information Risk Experts Committee (IREC) channels.

Threats extend to target all sectors (see Figure 5). Threat analysis showed a relatively high percentage of infections in the education (17%), followed by hospitality (12%), and then construction (7%).

---

\(^3\) The TMS data is indicative as it is dependent on the limitation and accuracy of the received feeds.
The highest threat detected on the system in 2014 was spam, which originated from computers in Qatar, with a number of 72%. Computers that send spam are most likely to be infected with malicious software. Following spam as a source of detection, malware is the second highest detected threat holding 25% of the total number. Systems are infected by malware due to vulnerabilities and loose security controls (see Figure 6).
While it is not a new threat, Conficker malware is still propagating in Qatar and dominating the chart with 54%, followed by Zeus families, the infamous banking malware, and Sality malware (see Figure 7).

![Malware families](image)

Figure 7: Malware families collected from all feeds in Qatar

B. Weekly Newsletter
The Cyber Security Team prepares and distributes a public weekly newsletter email that covers the global cyber security landscape. It is a tool used with the goal of keeping information technology and security professionals updated with cyber threats, incidents, tools, analysis, reports, guides, and any others related topics.

In 2014, the Cyber Security Team distributed 50 newsletters to 950 subscribers from 35 countries with the highest percentage of subscribers (83%) being from Qatar (see Figure 8).

The subscribers from Qatar come from a wide range of sectors with the government being the highest (35%) followed by energy (20%) and telecom (18%). (See Figure 9)
C. DNS Log Analysis

Domain Name System (DNS) logs refer to all the communications exchanged between the machines on a certain network with its local DNS server. The DNS log analysis platform is a tool developed by the Cyber Security Team, which is a pioneer in providing this service to Qatari constituents, by using open source infrastructure. The purpose of DNS log analysis is to detect suspicious or malicious Domain Name requests from internal machines using heuristics and statistical analysis of internal DNS logs utilizing big
data tools. The analysis provides indicators to the compromised machines on a certain network. The findings then forensically analyzed when requested to gain more knowledge of infections. This analysis is done offline using the data provided by the organization who requested the service.

In 2014, the number of DNS log entries that were analyzed reached 600 million records for more than 20 analysis cases. An average of 20 malicious internal machines was detected per organization.
3. Cyber Security Resiliency

As cyber threats have become more sophisticated and destructive, there is a need to consider cyber security from a different perspective. Cyber security emphasizes on protecting organizational information assets from cyber threats and attacks. Cyber Resiliency is a strategic approach that can be described as an organization ability to function properly and securely despite disruptions to its information systems. The cyber resiliency approach is gradually being recognized as an important component of comprehensive cyber security practices.

The Cyber Security Team provides organizations in Qatar with proactive measures to ensure having secure and resilient information systems.

The Cyber Resiliency was able to accomplish many vital goals through its mission to ‘Lead in innovative and effective approaches for implementing, evolving and improving maturity of cyber resiliency in national organization’.

Cyber Resiliency developed its own Technical Security Assessment Framework, which is derived from international standards and methodologies such as NIST, OWASP and others. Based on that framework, a number of technical and governance assessments can be offered to constituents including: vulnerability assessments, penetration testing and initial vulnerability scanning. New governance assessment services were developed and launched in 2014 such as Network Design Review (NDR) and National Information Assurance Baseline Assessments (NIABA).

Eighteen technical security assessments were conducted to critical sector organizations in 2014 (see Figure 10). The highest number of assessments was for vulnerability assessment with 53%, followed by penetration testing with 27%. These numbers rely on the demand from constituents to these services. Moreover, the Cyber Security Team conducted special projects to verify compliance and alignment with the National Information Assurance Policy (NIA) such as conducting Physical Security Assessment of a Data Center facilitator.

![Graph showing distribution of security assessments]

Figure 10: Cyber security assessments in 2014

---

4 This number indicates the number of engagements and does not indicate the number of assessed systems.
The conducted technical security assessments are represented in terms of the vulnerabilities found on those systems and categorized as: web server vulnerabilities, web application vulnerabilities, vulnerabilities in secure sockets layer (SSL) certificates and others (see Figure 11). The technical security assessments represented focus on online services such as websites, web portals, mobile applications and others. The numbers found indicate a need to focus more on Web Application Security.
4. Public Key Infrastructure Licensing and Identity

Digital certification services and digital signatures based on Public Key Infrastructure (PKI) technologies can enable citizens, residents and corporates to conduct electronic transactions securely. Digital signatures and related services will ensure Integrity, Confidentiality, Authenticity and Non-repudiation.

In 2010, Qatar enacted the E-commerce and transactions law no. 16 of 2010, which mandates the Ministry of Information and Communications Technology to regulate electronic signatures and digital certification in the state. The Ministry in this regard represents the Policy Management Authority (PMA), which is the entity responsible for licensing and supervising certification service providers in Qatar. PMA also manages the National Root Certification Authority (NR-CA) and, due to the absence of a national accreditation body in Qatar, PMA will play the role of Conformity Assessment Bodies Authorizing Authority (CABAA). PMA, as well, is responsible for encouraging the international recognition of the Qatari NR-CA and the approval of foreign certification services through cross-certification.

The PKI section had received the first application of a Certification Service Provider, audited the applicant through a third party auditor, and reported the final report to both PMA steering committee and the minister.

The Ministry of Information and Communications Technology had issued the digital certification policies that all licensed CSPs should abide by its requirements.

In December 2014, H.E. Dr. Hessa Al-Jaber, the Minister of Information and Communications Technology had issued the first Certification Service Provider License to be issued in the State of Qatar. The License is issued to the Ministry of Interior which is, as a CSP Licensee authorized, to provide all necessary services, including the maintenance of a public keys' infrastructure for, the providence of services related to electronic signature and the issuance of digital certificates.
5. Cyber Security Training and Awareness

The Cyber Security Team strives to nurture an information security workforce with the required skill set by providing information security competency and capability building mechanisms. This is efficiently accomplished through internal competent capabilities and strategic collaborations with reputable organizations and internationally accredited institutions.

For most organizations, developing and maintaining a competent cyber security workforce is a fundamental requirement to ensure resilient operations. The rapid change and dynamic nature of the cyber security field makes it challenging for organizations to guarantee that their cyber workforce possesses the most relevant and current knowledge, skills, and experience.

Working with stakeholders, the team has developed solutions to help organizations achieve dramatic improvements in their cyber workforce development programs. The team provides organizations with technical programs and awareness content needed to develop and maintain a competent, skilled, and effective cyber workforce.

The Cyber Security Team identifies target areas where constituents require additional information and guidance in order to enhance their protection against cyber-attacks. One of the core activities includes promoting security skills through structured general cyber security awareness programs and delivering cyber security training courses with the best practices guidelines and advisories.

During 2014, the team successfully held 5 technical and management information security courses through its partnership with SANS institute. Those courses mainly targeted government entities and critical infrastructure organizations. The total number of attendees in the provided courses was 107 with 75% of them being Qatari Nationals and 67% of the total number were from the government sector (see Figure 12 and 13).
Figure 12: The number of training attendees in 2014

- Finance sector
- Energy sector
- Government
- Universities

Figure 13: Number of training attendees per sector

Information Security Risk Management is a systematic approach to identify organizational needs in information security and address risks in an effective and timely manner, where and when, they are needed. Information security risk management is an integral part of all information security management activities.

Information Security Risk Management is a continual process to identify, assess, treat, communicate, report and monitor the information security risks. Before attempting to make business decisions, risk management analysis is an integral part to simulate what can happen and the possible consequences all in an effort to reduce risks to an acceptable level.

A. Information Security Risk Management Framework

To better support constituents and organizations in Qatar, the Cyber Security Team has developed the Information Security Risk Management Framework\(^3\). This framework is a structured yet flexible approach that can be aligned with the overall risk management framework of an enterprise. It provides the agencies with a systematic approach to identify, prioritize, and manage information security risks and to comply with the requirements of the National Information Assurance Policy (NIAP).

The methodology behind the framework is formed from the phases of the Risk Management Program lifecycle which are: risk identification, risk assessment, risk treatment, risk communication, and risk monitoring. Each phase contains various activities covering input, procedures, guidelines, output and roles and responsibilities (see Figure 14).

\(^3\) The information risk management framework is available upon request from the Cyber Security Team.
Figure 14: Information security risk management Framework Methodology

An in-house toolkit was developed and provided within the framework to optimize the information security risk management processes for organizations (see Figure 15). This tool drives efficiency into the risk management process, while providing the business with a more defined view into information security risks (see Figure 16 and 17).

![Screenshot of the toolkit](image-url)
B. Specialized (on-site) Critical Infrastructure Security Assessments

The team continues to conduct on-site visits to assess and provide security advice to operators of mission critical systems such as Industrial Control Systems (ICS) owners and operators, using the National ICS security standard as the security benchmark. The team conducts plant network architecture review, risk assessment and gap analysis and provides technical recommendations on how to improve the security of the critical information infrastructures. In 2014, the team completed 5 on-site visits covering: oil and gas, water and electricity producers as well as heavy industry manufacturers raising the total to over 30 on-site assessments since 2010.
C. ATM Security Guidelines

Handling Automated Teller Machine (ATM) properly is a critical component in a financial institution's risk management strategy. The compromise of an ATM can result in a wide-scale theft of personal identification numbers (PINs), fraud, and serious damage to an institution's reputation and the loss of customers' confidence in the ATM network and consequently the financial institution itself.

To address the risks associated with ATMs, the Cyber Security Team drafted ATM Security Guidelines\(^6\) with the contribution of the Financial Sector Information Risk Experts Committee (FS-IREC)\(^7\) members proposing a set of controls necessary to mitigate the risks associated with the attacks targeting ATMs (see Figure 18). FS-IREC members can request on-site assessments for ATM machines and networks.

1. Hardware Security [PC.HS]

   **PC.HS.1** All the ATM components should be encapsulated within the ATM’s outer shell, including wires and all the different components of the ATM.

   **PC.HS.2** The ATM should be equipped with at least one of the following anti-skimming methods:

   - A device to prevent the attachment of a card skimmer on the card reader module.
   - A device that is able to detect the installation of a card skimmer.
   - A device that will jam any card skimmer, preventing the skimmer from recording the data.

2. Environment Security [PC.ES]

   Figure 18: Sample of ATM Physical Controls

---

\(^6\) The final version will be published in 2015.

\(^7\) Information Risk Experts Committee (FS-IREC) is an initiative by the Ministry of Information and Communications Technology to form sector specific public private partnerships (PPP). IRECs provide a trusted platform for sharing security challenges, anonymized incidents and lessons learned amongst stake holders of common interest. Since 2010 the Cyber Security Team has established Energy, Finance and Government sector IRECs.
7. Cyber Security Crisis Management

Cyber Security Crisis management is a tool to assist critical sector organizations to deal with major events that threaten to harm organizations, stakeholders, or the public.

Sophisticated cyber-attacks, high profile data disclosures and acts of hacktivism are some of the growing risks that organizations face. Those risks can affect organizations by significantly impacting business operations and shareholder trust. Hence, the rapid and effective reaction from the organization toward the crisis is crucial. It can be the fine line between recovering well, or not at all.

The Cyber Security Team in the Ministry of Information and Communications Technology has taken a consultative approach to help organizations quantify and qualify their exposure to cyber threats, business continuity management and emergencies. This approach ensures that critical sector organizations have the most appropriate and effective crisis management strategy.

Cyber security crisis management provides three core services:

- Establishing process used to respond to both the reality and perception of cyber crises.
- Establishing metrics to define what scenarios constitute a cyber-crisis and should consequently trigger the necessary response mechanisms.
- Creating effective communication channels in the response phase of cyber emergency-management scenarios.

The Cyber Security Team ensures crisis management in terms of readiness of critical sector organizations by conducting cyber security exercises at sector and national levels.

A. Qatar’s National Cyber Security Drill

A cyber drill is an exercise along the lines of cyber security workforce and process development. It focuses on creating proper levels of readiness against cyber threats with an objective to verify, test and improve national level communication, coordination and collaboration at the time of cyber-attacks or crisis situations. The exercise simulates different attacks that target organizational and national infrastructures putting the participants in a reactive cyber defense modus operandi to protect those assets. The Cyber Security Team plans an annual cyber drill to strengthen core process areas like Incident Response, Business Continuity, Risk Management and Crisis Communications (PR) for critical sector organizations such as the government, energy, finance, communication, health, utility, education and transport. It is a practical exercise that creates an opportunity for participating organizations to test and improve internal procedures, establish interagency collaboration and provide feedback to enhance the national cyber crisis readiness.

The Cyber Security Team has planned a series of cyber drills. The first one, code named Star-1, was conducted in year 2013 with the objective to institutionalize the fundamental knowledge of incident handling, crisis communication and situational awareness among critical sector organizations. After the
success of the first exercise, a more holistic one, code named Star-2, was organized on December 15, 2014. Star-2 brought together 34 participating organizations from the government, financial, Energy, Healthcare, Transportation, Utility and Telecom sectors (see Figure 19).

![Figure 19: The number of participants in Star-2 per sector]

Collectively 180 management executives and over 300 technical professionals participated in this one-day event. The participant’s roles ranged from middle to senior managers from risk management, information security and critical (plant) operations.

During preparation, intensive research was conducted to decide on the best approach that focuses on the national needs and delivering the required objectives. That led the team to select a blended approach consisting of tabletop exercise coupled with technical hands-on in a controlled environment. This unique approach enabled the participants to focus on both management and technical aspects simultaneously and provided a comprehensive environment for organizations to test their end-to-end readiness. To ensure maximum benefit, organizations were exposed to sector-specific situations that would enable them to practice and self-evaluate their critical business processes including: information (IT) security, business continuity and disaster recovery, risk management, situational awareness and crisis management. The no-score based methodology and transparent reporting mechanisms created a trusted environment for organizations to volunteer for participation. More than 50% of organizations participated for the second time. The event witnessed significant participation from government sector, with almost 150% increase from the previous exercise.

The participating teams were presented with challenging scenarios that were twined across multiple sectors to demonstrate inter-dependence and importance of mutual communication. The scenarios
included situations of public credential disclosure, fraudulent mobile transactions, malware and vulnerability management, email related threats, system destruction, service unavailability and mission critical assets unavailability.

During the event, the management team in the tabletop format focused more on the strategy and the business side of the situation and the technical team was conducting the practical side of security operations on the virtual machine infrastructure, which was specifically created for the exercise. Towards the end, the multiple teams from different organizations were sharing information and collaborating as one unit. Many participants were able to test their internal processes and identify areas of improvement.

8. Cyber Security Information Assurance

Information and technology used to access, utilize, store, and transfer knowledge are the primary factors of prosperity in today's global digital economy. However, the use of technology by itself tends to be susceptible to cyber security issues in many aspects, and especially when exposed to open networking environments such as the Internet.

Information security is not only a technical issue, but also a business and governance challenge that involves risk management, reporting, and accountability. It is a top-down process that requires a comprehensive information security strategy that is explicitly linked to an organization's business processes and objectives.

Information Assurance is the practice of inspiring confidence in the use of technology and ensuring recovery and business continuity in the event of a cyber-incident. Information Assurance is an interdisciplinary approach requiring knowledge and expertise in fields such as business management, accounting, systems engineering as well as computer science.

The information security threats that Qatar faces are diverse and evolving. In 2010, the Cyber Security Team has developed the National Information Assurance Framework (NIAF) as a comprehensive and good-practice-setting model. NIAF provides standards that are designed to be mandatory as well as guidelines under which Qatar's information posture thrives. The guidelines provide information and direction for the practice of information security and assurance.

The Cyber Security Team continues to succeed in pushing for the implementation of the National Information Assurance (NIA) policies and standards by offering compliance aid and professional consultations to organization in Qatar.
An accreditation and certification framework was developed to approve and accredit qualified certification agencies to audit and certify state agencies against all National Information Assurance policies and standards. The framework will be implemented in 2015 with the aim of creating an ecosystem for compliance.

The Cyber Security Team in participation with the Ministry of Information and Communications Technologies' legal legislative committee proposes drafts and reviews cyber security related laws such as the Data Privacy law and the Critical infrastructure Information Protection law. Both laws have been approved by the Cabinet in April 2014 and pending final endorsement.

The Cyber Security Team worked with international and local security companies and has successfully included the NIA security controls as a recognized and integrated standard model available in the most popular Governance Risk Compliance automated tools.
9. Cyber Security Policy and Standards

Through new and improved technologies, our lives have been enriched with the ease of communication and the vast amount of data and information we can reach with the touch of a button. However, this ocean of information and the systems that lies within need to be properly governed to avoid the misuse of critical information. Policies and standards are two of the main vehicles to achieve governance and ensure compliance.

The Cyber Security Team had a memorable year as it participated in drafting Qatar’s National Cyber Security Strategy and ensured that the various critical information infrastructure protection functions and programs are aligned to the nation’s strategic goals and objectives. The team had also successfully published the following policies and standards in 2014 completely relying on the internal resources and subject matter experts:

- **The National Information Assurance Policy (version 2.0):** This document is the flagship of information assurance in Qatar. It is the nation’s standard in information security. A revised and updated version 2.0 was released this year.

- **The National Industrial Control Systems Security Standard (Version 3.0):** The standard is developed for critical organizations that operate Industrial Control System (ICS). The functioning of many critical utilities such as water and power depends on automated systems and critical computer networks. These critical information systems need to be protected to ensure a secure critical infrastructure which can sustain the nation’s development. Upon issuance of the critical information infrastructure protection Law, compliance shall be mandatory, however many oil, gas, electricity and power companies in Qatar are already implementing the guidelines. Although it is a national standard, it was globally recognized in a recent survey conducted by SANS institute\(^8\) in April 2014 that resulted in rating it amongst the most recognized ICS standards globally.

- **The Information Security Framework for Educational Institutes:** This framework summarizes a set of standards that ensure a more secure educational environment. The document includes policies and tools that can be used by educational institutes to improve the security posture of their technical platforms without limiting the experimental spirit of students.

- **Guidelines For Incident Management Pre-Requisite Measures:** The Cyber Security Team published the guidelines for all organizations to assist in building a solid foundation for incident management capabilities, including processes and technical controls. The availability of these processes and controls will assist organizations and their incident response teams during cyber incidents.

- **Broadband Infrastructure Security Policy:** The Internet Security guidelines published in 2013 have been updated and superseded by the Broadband Infrastructure Security Policy. The policy

had been approved and published in 2014 and was issued for broadband service providers to specify the minimum security baseline that should exist to ensure resilient networks.

- **The Accreditation and Certification Framework**: The document proposes a framework to drive and monitor compliance of cyber security policies within organizations in Qatar. The framework aims to motivate organizations to comply with cyber security policies by providing a mechanism of certification and tools to the Ministry of Information and Communications Technology to monitor the compliance of cyber security policies within an organization, and providing guidelines to accredit external audit companies to play the role of certification bodies thereby enabling the market and building local capacity.

- **Government Cloud Security Policy**: The policy is aimed at government agencies that use or intend to use cloud services. Cloud computing brings major cost benefits, but also introduce confidentiality risks. The policy is designed to control the risks associated with sharing government owned data in the cloud and provide a criteria on how government agencies may choose the best cloud solution from a security perspective.

## Memberships

**International Memberships and activities**

- Voting member in IEC/ISA 62443 international standards
- Committee member in the Meridian Process ([www.meridian.org](http://www.meridian.org))
- The Policy and strategy initiative to host an international library for all critical infrastructure information protection (CIIP) related materials from around the world continues to be a great success; several countries are now contributing to the international library ([http://www.qcert.org/meridian-library](http://www.qcert.org/meridian-library)).
- Member of ENISA, OWASP, APWG and other specialized organizations for international collaboration.

**Regional Relationships**

**GCC-CERT**

The GCC-CERT was established by the decision of the Gulf Cooperation Council in May 2006 to address the topic of information security incident handling in the Gulf region. The GCC-CERT initiative is derived from the GCC Charter objectives that support effective coordination, integration and inter-connection between the Gulf Council Member States in terms of scientific and technical progress in various fields and establishing scientific research centers.

### A. Local Relationships

Information Risk Expertise Committees (IRECs)
Q-CERT as a trusted government entity will identify and facilitate the establishment of work groups (IRECs) within critical sector organizations in Qatar. These trusted forums provide additional information, collaboration and partnership opportunities to help protect critical sectors from cyber threats and attacks. Work groups are created to focus on sector specific challenges. Q-CERT is working with the Financial sector (FS-IREC), Energy sector (EN-IREC) and government sector (GOV-IREC).