QCRI Emerging Cybersecurity

Threats in Qatar and the Middle East, 2015

معهد قطر لبحوث الحوسبة
Qatar Computing Research Institute

عضو في مؤسسة قطر
Member of Qatar Foundation

QCRI Emerging Cybersecurity

Threats in Qatar and the Middle East, 2015

معهد قطر لبحوث الحوسبة
Qatar Computing Research Institute

عضو في مؤسسة قطر
Member of Qatar Foundation

QCRI Emerging Cybersecurity

Threats in Qatar and the Middle East, 2015

[prepared by]

Robert Lemos
Lemos Associates LLC
P.O. Box 552
Barrington, NH 03825
USA

Mustaque Ahamad
Georgia Tech Information Security Center
Klaus Advanced Computing Building
266 Ferst Drive
Atlanta, GA 30332-0765

Designed and printed by Digital Print House (DPH) - QF Publishing Center (QFPC)

Table of Contents

letter of introduction

Over the past year, numerous incidents, breaches and attacks have thrust cybersecurity into the limelight. The number of attacks — as well as the velocity and ferocity of the incidents — has continued to grow both globally and regionally. Espionage operations against targets in the Middle East have resulted in stolen data and compromised privacy, attempts to disrupt services in Qatar through denial-of-service attacks are increasingly common, and hacking social-media accounts has become the tool of choice for propagandists and protesters.

Unfortunately, defensive technology and processes have not been deployed or, if deployed, are not being used to their fullest potential. Despite an increasing level of investment in and effort focused on cybersecurity, companies and government agencies continue to have trouble protecting both their users and data. Hardly a month goes by without the detection of a massive breach of consumer data somewhere across the globe or the discovery of a far-reaching espionage operation focused on gathering intelligence on governments and companies. In December 2014, for example, one security firm released a report on an espionage network that targeted, among others, Qatari companies and government agencies.

These events underscore the need for deeper analysis of cybersecurity trends, more comprehensive research into possible defensive measures and policies, and increased investment in countermeasures by stakeholders. Research into attackers' methods can inform both the creation of technical countermeasures and the formation of better policies designed to protect critical infrastructure and citizens' data. Self-healing systems, for example, hold out the promise of more effectively combatting breaches, while additional layers of virtualization and defenses could keep potential threats away from critical data. On the policy side, better information sharing, such as a global exchange for data and information among defenders, could better help protect systems.

Qatar has already embarked on a number of significant initiatives to secure its digital future. In 2013, Qatar established the National Cyber Security Committee, which has formulated, and will continue to create, national priorities for protecting data and systems from attack. In March 2014, Qatar's Ministry of Information and Communications Technology published its second version of the National Information Assurance Policy, which outlines the requirements and responsibilities of critical-infrastructure firms to secure their networks.[1] Qatar is also the first country to partner with INTERPOL on a national cybersecurity assessment, an effort that will help improve information sharing and law enforcement's ability to investigate cybercrime.

> National projects and initiatives such as healthcare, the preparations for the 2022 FIFA World Cup and Qatar's commitment to the creation of smart cities will make such efforts even more important.

In support of those efforts, Qatar Computing Research Institute (QCRI) continues to research the cybersecurity threats facing stakeholders and find solutions to the technical issues posed by such threats. Tackling such large-scale, complex computing challenges has been our mission since the institute was established in 2010 by Qatar Foundation for Education, Science and Community Development. Our vision is to become a global leader in areas of computing research that will bring a positive impact to the lives of citizens and society. We conduct innovative, multidisciplinary applied computing research that addresses national priorities by enhancing the quality of life for citizens, enabling broader scientific discoveries and making local businesses more competitive globally.

> With cybersecurity designated as a national grand challenge, we are pursuing a variety of research initiatives and collaborating with universities and research centers worldwide to inform national policy and create a more resilient information infrastructure.

This report presents the current threat landscape and aims to create a foundation for the national discussion on how organizations can defend against and mitigate cybersecurity threats.

Research into cybersecurity issues and challenges is one of our major missions. In 2013, we brought together local and international experts with Qatari stakeholders—such as local universities, media organizations, energy companies and the Qatar Ministry of the Interior—to discuss cybersecurity in Qatar and to determine a framework for establishing a cybersecurity research center. The following year, we issued the first annual Emerging Cyber Threats report for Qatar and the region.[2]

This latest report discusses the emergence of unique facets of current cyber threats and the continuing challenges posed by threats identified in last year's report. While the threats largely remain the same, QCRI hopes the reports will provide the basis from which Qatar can foster an open discussion of cybersecurity, the potential impact of these threats on the country and region, and the development of defenses for containing them.

Signed,

Dr. Ahmed K. Elmagarmid
Executive Director

Overview

In 2008, the government of Qatar established a National Vision, committing to human, social, economic and environmental development for its people. A key factor in the National Vision is the creation of a diversified and robust economy by 2030,[3] comprised of innovative and knowledge-based businesses effectively using information and technology.

Qatar has made significant progress in its technology goals, but security threats represent potential pitfalls for its efforts. In the year since the release of the previous report, the cyber landscape has changed significantly.

> Initiatives such as the Msheireb and Lusail smart city projects, the increasing digitization of medical records, and the monitoring and control of numerous devices — often called "the Internet of Things" — has intertwined the digital and physical worlds more tightly than ever before, promising great dividends.

One measure of national progress, Qatar's information and communications technology sector, has grown an average of 17 percent per year and, by 2016, is on target to deliver broadband with 100 Mbps download speeds to 95 percent of households and broadband speeds of 1 Gbps to businesses, schools and hospitals. In 2013 and 2014, the country ranked 23 in the world[4] on the global Network Readiness which currently ranks 148 countries in terms of the potential for their businesses and citizens to take advantage of the information and communications technology. In 2007, the country ranked 36th.[5]

> **The quick progress highlights Qatar's advantages. A rich resource base, relatively small population and dynamic economy allow the country to quickly grow and take on new challenges with agility,**
>
> said Dr. Soumitra Dutta, Dean and Professor of Management and Organizations at Cornell University's Johnson Graduate School of Management.

"Qatar is able to do things at a faster pace than most other countries," he said. "But there are risks that come with growth and the adoption of technology at such a fast pace."

Information and communications technologies (ICT) enable new economic models but at the same time invite cyber attacks and cybercrime. Online services allow businesses to offer new products to consumers and the government to better serve its citizens, yet also create the possibility that a variety of actors — from rival nation-states to hacktivists — could disrupt critical services. Because the digital world increasingly intersects with citizens' lives, attackers have access to more data on citizens and, with the increasing adoption of connected devices, access to the things in their lives as well.

This report focuses on the issues and threats that enable attackers to compromise and disrupt digital systems. The lack of information sharing between stakeholders and the shortfall in workers with cybersecurity skills leave companies and government agencies at a disadvantage when defending against more advanced attacks. The difficulty in guaranteeing the security of acquired infrastructure, and the subsequent protection of that infrastructure, puts critical systems at risk. And, with the growing sophistication of attackers and their techniques, defenders must work harder to protect an ever-growing collection of digital devices, networks and systems.

As Qatar creates a more knowledge-focused economy, businesses and infrastructure should be made resilient against the evolution of these threats. Critical infrastructure needs to be secured, and as businesses and consumers adopt more connected technology that communicates directly to the Internet, efforts must be made to secure that technology as well.

Knowledge and a trained workforce are necessary to combat these threats. Spending on current technology will not deliver the defenses the nation needs. Globally, attackers continue to have the upper hand, despite enormous spending on security technology and services. Countries should continue to pursue an aggressive research agenda that reveals new ways to secure infrastructure, protect citizens' data and detect and remove threats.

"We need to focus on how we can get ahead of the game," said Dr. Ahmed Elmagarmid, Executive Director of QCRI. "Our thinking in cybersecurity has been fairly mundane and fairly archaic. We need to think outside the box."

Qatar has embraced the challenge, however. The national government has already established the National Cyber Security Committee to set priorities for cybersecurity, created a National Information Assurance Policy, and is the first country to partner with INTERPOL on a national cybersecurity assessment.

"If we have this discussion this time next year, I expect things will be quite different from how they are now," said Steve Honiss, National Cyber Review Manager at INTERPOL's Global Complex for Innovation (IGCI). "Qatar sets itself apart with its ambitious plans and aspirations for a really digitized economy."

> The global cybersecurity market will grow from an estimated US$71 billion in 2013 to US$155 billion in 2020, representing a compound annual growth rate of 11.8 percent, according to Frost & Sullivan.[6]

Lack of visibility into threats and attacks hinders cybersecurity planning and operations

While Qatar has embarked on information-sharing initiatives, businesses and government should collaborate more to quantify and understand the threats.

Highlights

- Companies lack adequate visibility into the use of their networks and data, leaving attackers able to operate in stealth.
- While some critical sectors share data on attacks and threats, most companies do not have intelligence on the threat landscape.
- The general public continues to lack understanding of the impact that cyberattacks could have on their lives.
- More information-technology workers trained in cybersecurity and governance processes are needed to help defend the nation's data and networks.

Security professionals and government officials in Qatar are hindered by a lack of data on the threats currently impacting the country's infrastructure and businesses. Many groups — from network operators to corporate information-security departments to government agencies — have a piece of the overall picture, but information about threats is infrequently disseminated beyond a few small groups.

> **"Clearly, we are not sharing information even at the national level,"**
>
> **"We don't have an overarching mechanism by which we share information."**
>
> said QCRI's Dr. Elmagarmid.

Problems with information sharing is not an issue unique to Qatar. Nearly, every country's public and private sectors are reticent to share threat data. The United States, for example, has struggled to pass a law that gives companies who share attack information legal protection against lawsuits.[7]

Qatar has taken several steps to encourage the sharing of information between authorized groups. In the National Cyber Security Strategy, the collection of data on threats and the sharing of attack information has been designated a top objective.[8] In addition, the country has established three Information Risk Expert Committees (IRECs), which exchange information between businesses and government agencies in the energy, finance and government sectors. And, in December 2014, the country conducted its second national cyber exercise with more than 300 participants from the banking, energy, government and transportation sectors.

Yet, more needs to be done. While attackers often share offensive techniques online, defenders continue to remain mostly quiet about their experiences defending systems and fending off attacks.

Companies lack visibility into anomalous network activity and use of data

A variety of threats are impacting systems within Qatar, but few studies exist to define the scope of the problem. An exploratory research project conducted by QCRI found that the ZeroAccess botnet had infected more than 100 PCs inside the country. In a second study conducted by university students, thousands of other infections were found in the nation's systems.

Without better data on the types of threats and their impact, government agencies and companies will not be able to make informed decisions on how best to defend Qatar's networks and data. The Shamoon attacks against oil-and-gas firms Saudi Aramco and RasGas in 2012 underscored the vulnerability of those networks.[9] Yet, a similar campaign in 2014, dubbed Operation Cleaver,[10] compromised companies and government agencies in 16 countries, including four organizations in Qatar, without detection.[11]

> "The principal threat we are facing is not the groups or the growing attacks on businesses' reputation or financials," said Ali Majid Al Hashimi, IT Governance & Standards Manager in the Information Technology Directorate at Qatar Foundation. "The growing threat is the lack of awareness and preparedness of organizations to counter these attacks."

Companies and government organizations continue to approach the problem in a reactive way. A more proactive approach is necessary, including the creation of a national database of security incidents, the sharing of threat intelligence between businesses and the government, and the creation of resources for aiding in the analysis of attacks.

"It is a lot of work and, it is not easy," said Faisal Al Kuwari, Chief Technology Officer of managed IT services and hosting firm Meeza.net. "When you are in security, you are as secure as the technology, people and processes. There needs to be adequate investment and senior management support in order to get it right."

Failure to widely share intelligence on threats will hinder defenses

Qatar has already made progress in sharing information on threats among key industry and government players through the creation of the aforementioned IRECs and through conducting two cybersecurity exercises, with 30 organizations from the nation's critical sectors taking part in the most recent exercise.[12]

Yet, only the largest firms tend to benefit from such information-sharing regimes. In the United States, for example, the Financial Services Information Sharing and Analysis Center (FS-ISAC) tends to mostly benefit the largest banks. Smaller financial institutions and related industries — such as credit-card processing firms — have created their own information-sharing groups to serve their specific needs.[13]

Companies should find ways to more widely share threat intelligence. Without information sharing, the cybersecurity equation shifts to favor the attacker.

> **"All organizations should have a threat-based incident response and should work on this area,"**
>
> **"Otherwise, with the right amount of money and time, attackers will eventually break in."**
>
> said Mustapha Huneyd Bengali, Corporate Information Security in the Office of the CEO at Ooredoo.

Private information exchanges could help. Numerous threat-intelligence sharing forums have been created worldwide. IBM, for example, has launched the X-Force Exchange, allowing more than 1,000 organizations in 16 industries to share information on threats and help each other be prepared for attacks.

> "Participants in the exchange are able to: validate research findings, share a collection of indicators of compromise (IOC) to aid in forensic investigations, and add context to threats through peer collaboration," said Dr. Tamer Aboualy, chief technology officer for IBM Security's Middle East and Africa division.

Lack of security knowledge hindering the defense of businesses and consumers alike

Combining data with other information about attackers and their tools is necessary to generate actionable threat intelligence. Yet, without knowledgeable and skilled IT security practitioners, even a clear picture of threats will not result in better defenses. More than 2 million IT security positions will need to be filled by 2017, with organizations in the Middle East suffering the skills shortage most acutely in security leadership positions as well as auditing, testing, forensics analysts and incident handling.[14]

The shortage in information-technology security professionals is a global problem, but one that impacts Qatar acutely. "The lack of qualified, skilled professionals makes the country vulnerable to all kinds of threats," said Osama Kamal, Cyber Threat Intelligence Section Manager with Qatar's Ministry of Information and Communications Technology.

The need for education and cybersecurity skills is not limited to IT security professionals. Citizens and consumers need to be more aware of the impact of cybersecurity threats on their lives.

A study[15] shows that MENA users seem to be among the most careful while online, with 45% of them saying that they "totally agree" with the statement "I am very careful about what I do or say on the Internet". Nevertheless, compared to worldwide averages, the same survey reveals that users in the Middle East are more likely to engage in what could be risky online behavior, such as opening attachments and documents from senders they do not know. At the same time, they are less likely than the average user to have antivirus and other security software installed to protect their data and ensure that their systems remain clean. In other words, these users think they are careful but their behaviors indicate another reality. Education and training can help solve these issues.

Mining Big Data to Find Threats

While convincing companies to part with data regarding attacks and probes is difficult, the payoff could be huge. QCRI is investigating ways to mine extremely large sets of network data using a variety of analysis techniques to find indicators of likely attacks.
For example, by using classification techniques and data from known attacks, researchers hope to find interesting patterns that could warn defenders of attacks that escape notice today, said Dr. Ting Yu, Senior Scientist at QCRI "We want to extract features to learn better classification, which could lead to the discovery of previously unknown attacks or the ability to predict future attacks,".

Attackers increasingly target critical infrastructure and the supply chain

Qatar has taken steps to protect the networks most critical to its economy, but attackers will continue to target infrastructure systems and the businesses that supply technology and services.

Highlights

- Qatar's rapid modernization of its information and communications technology infrastructure could result in missed vulnerabilities.
- As systems are hardened, attackers look to seed their operations by introducing vulnerabilities or Trojan devices into the supply chain.
- More regional attackers are appearing, and their attacks are growing more severe, targeting critical infrastructure.
- Improvement of the critical infrastructure security continues to be stymied by older legacy components that do not have the protections or secure design to operate securely in an increasingly connected world.

While the threats facing Qatar's critical infrastructure sector are similar to those facing other nations, Qatar's pace of infrastructure investment is far more rapid than most countries. In the transportation sector, for example, the country has invested billions of riyals to build a new seaport, upgrade road infrastructure, build a new state-of-the-art international airport, and construct a high-speed commuter rail system.

Such rapid infrastructure development poses issues for maintaining the security of the country's critical systems and networks, which have already been targeted by hackers. In 2012, RasGas was hit with malware, dubbed Shamoon, which deleted data and crippled systems. The attack had a much greater impact on Saudi Arabia's national oil giant, Saudi Aramco, which had to replace hard drives on tens of thousands of systems [16]. In 2014, a group of hackers, believed to be sponsored by a Middle East state, successfully attacked a variety of critical infrastructure firms linked to oil-and-gas production, including four major organizations in Qatar. [17]

> **"This infrastructure includes components and software that may be several decades old,"**
>
> **"But in a persistent and intensified fight, it needs defenses that can be continuously upgraded."**
>
> said Dr. Dimitrios Serpanos, Principal Scientist, QCRI.

The protection of critical infrastructure has already been deemed a priority by the Qatar government and designated as Objective 1 in the National Cyber Security Strategy.[18] In March 2014, the Ministry of Information and Communications Technology (MICT) released an update to Qatar's National Information Assurance Policy,[19] giving information-technology managers a process by which to classify their information-technology assets and rules governing the protection of those assets.

"We are creating the proper structure to handle all of these security issues," said Dr. Guillaume Salha, Head Systems Engineer for Security Architecture at Qatar Petroleum. "We have a risk approach, so we are reviewing the proper security design and the proper processes."

The rapid growth of infrastructure could leave the nation open to attack

In its effort to transform its businesses to compete in a knowledge-based economy by 2030, Qatar is rapidly modernizing and expanding its infrastructure. From smart city projects to the nation's push for ubiquitous broadband, the government aims to provide a modern, information-technology-centric society.

Yet, with the adoption of so many new technologies comes risk, as those who would attack Qatar or its people focus on the companies who supply the country. In other countries, the problem has already become clear. Leaked memos have revealed that intelligence agencies have focused on inserting technological backdoors, or implants, into products before they are delivered to their destinations.[20] In 2013, U.S. retailer Target was compromised through a vendor that supplied heating, ventilation and air conditioning services.[21]

Because Qatar is rapidly building out its infrastructure base, the threat will likely be more acute, said Omar Sherin, Department Manager for the Critical Infrastructure Information Protection (CIIP) Division in the Ministry of Information and Communications Technology.

"We are quick to buy and adopt new technology, much quicker than any other country," he said. "We need to give more thought on how to protect such things."

Unfortunately, securing information technology against a determined attacker is a difficult research problem. While source code reviews and technical analyses can find design defects, detecting potentially compromised products is a difficult task. Yet, Qatar has begun creating a testing lab to certify that product meet specific security standards.

"We don't want to end up with some contractors choosing cheap equipment," Sherin said. "This lab will help us evaluate the equipment and create a base line."

Regional attackers are becoming more numerous and conducting more severe attacks targeting critical infrastructure

Espionage groups have focused on infiltrating government agencies and businesses in the Middle East for some time. Yet, public attacks typically have been limited to dissidents and propagandists targeting social networks and Web sites. Disruptive attacks, such as the targeting of Saudi Aramco and RasGas, have been reported only infrequently.

Experts expect that to change. Attacks aimed at disrupting operations, deleting critical business data or stealing intelligence appear to be on the rise. One suspected regional group, the Desert Falcons, have targeted a variety of government agencies and companies — including critical infrastructure firms — in Palestine, Israel and Egypt, stealing more than a million files in a search for sensitive intelligence documents.[22]

Another group, profiled in a December 2014 report,[23] had stealthily compromised more than 50 companies and government agencies in 16 countries, targeting critical infrastructure firms, targeting airlines and airports, manufacturing, and military networks as well as oil and gas companies [24]. More than 75 percent of the companies were in the Gulf region, according to security firm Cylance, which wrote the report.

> **"The [Operation Cleaver] group was solely interested in compromising critical infrastructure companies,"**
>
> **the security firm that conducted the research and published the report.**
>
> said Jon Miller, Vice President of Strategy for Cylance,

Cylance notified companies because the firm believed that the eventual aim of the attack was to disrupt oil supplies. "All they wanted to do was maintain persistence," he said. "They did not tip their hat, and there is not a lot of value in hacking an oil company to maintain persistence, except to disrupt the oil."

Industrial control systems continue to lag in security

Industrial control systems have historically been designed for reliability, not to resist a determined attacker. As operational technologies become increasingly connected to information networks, and through them to the Internet, industrial systems become more exposed to malicious attacks. Many security researchers have focused on finding vulnerabilities in industrial-control and monitoring systems, finding more than 800 security issues in products used worldwide since the beginning of 2011.[25]

During this time, attacks targeting supervisory control and data analysis (SCADA) systems more than doubled from 2012 to 2013, and then again last year. [26]

Yet, the vendors of such systems have been slow to react to the problem. While the makers of such systems have begun to release patches, their time to develop updates is slow. Moreover, patching industrial control systems — designed to be distributed across wide geographic areas and to resist tampering — is not an easy process.

Until vendors and security engineers find solutions to such issues, the best course for critical infrastructure providers is to make certain that their operation technology is separate from their information technology. "There are not a lot of choices," said Mohammed Abu-Nejim, Head of Systems and Network Operations for Qatargas. "We need to restructure the services around the SCADA system using different technologies but not touching the core of the SCADA systems."

New security technology can help. For example, systems that are hardwired to only allow SCADA products to communicate out to monitoring systems, but not allow traffic to the devices, can effectively firewall off an operational network from potential attackers.

Ensuring that critical infrastructure does not misbehave

When attackers exploit systems, they typically cause the computers to behave in ways that are not anticipated. Researchers at Qatar Computing Research Institute have teamed up with the Computer Science and Artificial Intelligence Laboratory (CSAIL) at Massachusetts Institute of Technology to build systems that include models of the correct process behavior and then warn when they deviate from that behavior. These computers include a cognitive middleware system, dubbed ARMET, which detects events that indicate an attack, diagnoses the problem and decides the most appropriate actions to contain its effects and recover.

"The system will monitor embedded applications and industrial control systems, comparing their behavior with the specification to determine whether there is something going wrong and will enable recovery from attacks and random failures under continuous operation," said Dr. Dimitrios Serpanos, Principal Scientist at QCRI.

Malware and actors grow more sophisticated with an increasing diversity of goals

Cybercriminals and hacktivists increasingly attack Qatar targets, while data reveals an existing focus by espionage groups.

Highlights

- The most common sources of infections in the region are no longer flash drives or other local media, but the Internet.
- An increasing number of sophisticated groups are attacking targets in the Middle East region using malware, denial-of-service attacks and botnets.
- Because of the popularity of smartphones in the region, attacks against those devices are expected to increase, if attackers can successfully monetize the compromises.
- Cybercrime is a growing problem in the Middle East, and the resources of the Gulf region have made Qatar and other nations into attractive targets.

In the last two years, the number of attacks targeting regional businesses, infrastructure and government institutions has grown quickly. Computers in the Middle East have encountered as much as 40 percent more malware in 2014, compared to the previous year, according to security firm Kaspersky Lab.[27] In Qatar, specifically, the number of denial-of-service attacks seen by local network providers increased 20 percent in 2014, according to Internet provider Ooredoo.[28]

While the spread of malware and cyberattacks has a variety of roots, the rise of more sophisticated and destructive nation-state and cybercriminal attacks is concerning. In November 2014, Sony Pictures Entertainment discovered that its systems had been thoroughly compromised when a image displayed on the firm's monitors announced that hackers, calling themselves Guardians of Peace (GOP), had stolen the business's data.[29] The hackers deleted much of the information on infected systems, calling the action retribution for a Sony-produced movie that the attackers deemed offensive.

Whether the attack was a nation-state operation, the actions of a disgruntled insider or a hacktivism campaign, the dramatic damage demonstrates that attackers can reach across cyberspace and impact a company, organization or nation with whom they disagree. Until international norms on cyber operations are settled, nations, protestors and criminals will continue to use online attacks as the preferred way to take deniable actions.

"Cyber will be a manifestation of geopolitics, but in many ways it will be the harbinger first,"

said Tom Kellermann, Chief Cybersecurity Officer of Trend Micro and former risk analyst for the World Bank.

The attack on Sony — like the attacks on RasGas and Saudi Aramco — underscores the dangers of rogue actors in the cyber environment. While nations and people held responsible for the actions can make rational decisions based on strategic objectives, the actions of rogue groups — whether governments or individuals — are much harder to predict.

"'If these cyber actors can perceive an offensive movie as an existential threat, then we should expect them to behave in ways that we haven't yet anticipated," said Jen Weedon, Manager with security-services firm FireEye.

Social engineering becomes primary vector of compromise

For a decade, local media — such as USB memory sticks, CD-ROMs and disks — have represented the largest infection vector for systems in the Middle East.[30] Over the past year, however, the increased use of the Internet and increased attacker sophistication has led to the rise of different types of malware spread through social engineering, according to research from security firm Kaspersky Lab.

> **"Infections from the Internet have been massively increasing over the past year,"**
>
> **"The shift has resulted in new, more targeted types of malware becoming popular – banking trojans, spyware, keyloggers and adware."**
>
> said Ghareeb Saad Muhammad, Senior Security Researcher with the Global Research & Analysis Team at Kaspersky Lab.

As the Internet becomes the primary vector for attack, social engineering has become the method by which attackers compromise victims' machines. Social engineering includes simple techniques such as fake e-mail messages to more sophisticated techniques, such as compromising legitimate Web sites and infecting specific visitors with malware. Security firm Trend Micro estimates that there has been a six-fold increase in such attacks.[31]

Attacks focused on espionage and disruption may become more common

Many of the attacks on networks and systems in the Middle East originate from outside the region. About 5 percent of all advanced malware in the EMEA region targeted Qatar in the first half of 2014, according to security firm FireEye.[32]

Yet, an increasing number of regional groups is behind attacks against nations in the Middle East. The recently discovered cyber-operations group Desert Falcons, for example, appear to be native Arab speakers and have stolen more than a million documents from their victims, at least one of which is in Qatar.[33] The Syrian Electronic Army redirected requests for Qatari Web sites to pro-Assad propaganda in October 2013. [34]

"The landscape has really changed," said Shareef Ali Alsayed, Information Security Consultant with the Ministry of Interior. "We are now seeing much more sophisticated groups."

Along with increasing attacker sophistication in the region, two worrisome techniques are becoming more common. One dangerous trend is malware, such as the 2012 Shamoon attack against Saudi Aramco and RasGas which destroys data on its targets. Such "wiper" functionality also destroyed data during the 2013 intrusions into South Korean media firms and the 2014 attack on Sony Pictures Entertainment. The loss of data from Sony Pictures led to significant business disruptions, damages of at least $35 million and the ultimate resignation of the CEO.[35]

> **While well-prepared companies can recover from such attacks, the deletion of data can lead to significant business disruption because efforts to respond to the incident are slowed,**
>
> said Dmitri Alperovitch, Chief Technology Officer and Co-founder of CrowdStrike.

"With Sony, you had the perfect storm of theft and public leaking of confidential data and malware deletion of data," he said. "The attack will have business repercussions for years to come, and that is certainly a troubling development."

Another technique that makes attacks more difficult to detect and mitigate is the trend of not using malware but instead stealing and using administrator credentials to break into companies and pose as an insider. The tactic makes it harder to attribute the attacks, because there is no infrastructure or malicious code that can tie a specific group to the attack.

"We are seeing adversaries use malware-free intrusion tactics where they break in and steal credentials, and use administrator tools, not malware, to move around the network and steal information," Alperovitch said. "And that creates a real challenge for defenders, who have a 'find the malware' mindset."

Cybercrime, historically a problem for Western nations, has become more prevalent

> Cybercrime is becoming a more significant threat to Qatar and other Gulf nations. Users in the Middle East, in general, have encountered three times more banking trojans in 2014 compared to the previous year.[36] In addition, the banking trojans are now localized — written in native Arabic and posing as communications from local financial institutions.

"In the past, if you were a user in the Middle East, you might be infected by a banking trojan, but it would be okay, because the malware was not designed for the Middle East," Kaspersky Lab's Muhammad said.

About half of all cybercrimes are financially motivated, according to Ministry of Interior data.[37]

Another cybercriminals scheme, known as ransomware, where victims' hard drives are encrypted and the criminal sells the digital key, represents about 6 percent of reported cybercrime. While the technique is well known in Europe and North America, few consumers and workers have encountered it in the Middle East.

A more common danger is the online extortion, where a criminal will steal pictures from a victim's computer or online account, search for embarrassing images, and then blackmail the person into paying a monthly fee. Because many users do not understand how to keep their data secure, the crime has become fairly common, representing about 20 percent of all cybercrime, said Shareef Ali Alsayed of the Ministry of Interior.

"We will have very hard days ahead of us, because things are getting worse and people are not being careful," he said. "People are adopting technology and the latest software, much faster than understanding the risks and without putting controls around it."

Building a Virtual Lab for Malware

To understand who is attacking business and government networks in Qatar, security professionals need a virtual lab to test suspicious files for malware. Qatar Computing Research Institute is building a system that will be an open exchange and analysis platform.

"It is important to have that capability, that expertise in house," said Dr. Marc Dacier, Principal Scientist at QCRI. "We want to try to understand who is attacking us, and by building a platform that companies can use, we can share the intelligence with others."

Because much of the data is in private hands, QCRI needs partners to gain better visibility into attacks on the networks.

"To partner with local Internet providers would give us huge visibility in what is happening across Qatar," said Omar Alrawi, Senior Software Engineer with QCRI.

Adoption of connected technology increases economic opportunities, but poses privacy risks

Mobile connectivity, smart devices and the increased use of the Internet will put people's lives online, unless education and privacy protections are in place.

Highlights

- Qatar's rapid adoption of devices and technologies that connect to the Internet will make privacy an increasingly important issue.
- The Internet of Things will put citizens' lives online — especially as initiatives such as electronic medical records and smart cities become a reality — making strong security and more comprehensive privacy protection necessary.
- Monitoring and analyzing data on citizens can help protect society but poses privacy risks as well.
- The trend toward profiling citizens will continue, moving from understanding consumer behavior to influencing their behavior.

With more people using smartphones, communicating online, and using Internet-connected devices, a greater portion of our lives will be recorded and gathered online by third parties. Already, many companies are collecting the data. While the larger Middle East and North African region is less concerned with online privacy, citizens of Qatar and other member states of the Gulf Cooperation Council (GCC) are more likely to recognize the dangers of putting data online. [38]

> **"In the real world, Qatar's people are very privacy aware,"**
>
> **"But in the cyber world, there is still an undeveloped sense of privacy and they still share their information online."**
>
> said Dr. Mashael Al Sabah, Scientist at QCRI, who is currently conducting research at the Massachusetts Institute of Technology.

In Qatar, citizens are less concerned with government monitoring, but continue to worry about their privacy. About twice as many citizens in the Middle East are unconcerned with online communications being monitored compared to the global average (17% vs 8%).[39]

"Many of my students see surveillance as a necessary thing for security and something that the government should be doing," said Dr. Ryan Riley, Assistant Professor in the Department of Computer Science and Engineering at Qatar University. "But balancing that desire with their desire for privacy is complex."

The Internet of Things will provide plentiful data on consumers and make privacy issues more serious

Qatar is forging ahead as one of the leading nations for smart cities. In addition to infrastructure expansion in preparation for the 2022 FIFA World Cup, the nation is establishing smart cities, such as the Lusail project, from the ground up and integrating technology into the design. From traffic lights to power systems to waste management, such cities will be focused on using information technology to make urban management more efficient and effective.

Along with wearable computers and sensors, home automation, and computers embedded in other devices, such as cars, connected technology will create a future where citizens will be increasingly dependent on computers and will be creating digital tracks throughout their daily lives. Some 50 billion to 200 billion devices will be in use by 2020, according to estimates.[40]

"We need to ask what impact will these devices have — the good and bad — on the traditional way of life," said Dr. Jaideep Srivastava, Research Director, Social Computing at QCRI. "How this will play out is very much in the open. It is happening very fast."

While predicting the impact that such devices will have on society, the rapid adoption of the technology will spotlight the handling of personal data and make national policies more important.

Threat 4

Businesses focus on Big Data analysis could put personal privacy at risk

The ability to connect devices and allow people to access information everywhere holds great promise. Such analysis, however, can also leak significant information to the public, even if the data is anonymized. Studies of video usage, search-engine usage and other online activity have found that even anonymized research data, if there is enough of it, poses a privacy risk.

> "There are many cases that show that it is not trivial to prevent inferences of private information when you publish data about a group of users," Dr. Ting Yu, Senior Scientist at QCRI. "Attackers will try to correlate any data, even anonymized data, with other information to try to uncover private information."

While the government is creating a legal framework to implement privacy regulations, the ability of businesses to perform analytics on massive data sets — including the browsing habits or buying choices of Qatari citizens — will highlight new privacy risks.

Online analytics will move from understanding consumer behavior to influencing it

Because data on consumers constitutes such a valuable commodity in the business world, the collection of data and analysis of user habits will continue in the absence of stringent policies. A variety of Web services — from search engines to social media — collect information on their users, but at the same time create profiles of their customers, which they then sell as an additional revenue stream.

Companies have begun to go beyond just profiling users. In June 2014, Facebook and Cornell University researchers found that filtering out negative expressions resulted in more positive posts, and vice versa.[41] In other words, the authors showed how users could transfer their emotional states to others, electronically, via emotional contagion, leading people to experience the same emotion without their awareness. This result highlights the possibility to manipulate, online, people's minds by means of massive scale contagion via social networks. In a follow-up post, Facebook stated it had created more guidelines for such research in the future, but neither apologized nor promised to refrain from such manipulation in the future.[42]

"The next wave of assault on privacy is starting to show up with advances in artificial intelligence," said Dr. Ahmed K. Elmagarmid, Executive Director of QCRI. "A business could potentially manipulate the attitudes and reactions of users in order to alter their likes and dislikes, not just document and track their behavior."

There are already some indications that such manipulation is already happening, yet for censorship, not profit. Security firm Thinkst, which consults for Al Jazeera, went looking for media manipulation using "sockpuppet accounts," and found online forums where such accounts dominated the conversations.[43]

> **"You can trivially spot these bot armies in use already making sure that one side's comments get the lion's share of attention,"**
>
> said Haroon Meer, Consultant for Al Jazeera and Principal Consultant at Thinkst.

Ongoing Cybersecurity Efforts

Qatar has identified cyber security as one of the nation's top grand challenges. In 2014, the nation directed immediate research and development efforts to mitigate the threats of current attacks and find ways to safeguard data and the digital infrastructure of the future. Other high-priority challenges include water security, energy security and healthcare.[44]

As the previous sections have shown, the threats posed by cybercriminals, hactivists, and espionage actors on the Internet are not dissipating. Rather, they are becoming more acute. Cybersecurity is a cross-domain challenge that much of the nation's infrastructure relies on, or will rely on in the future. Qatar has created a solid policy foundation, including establishing the National Cyber Security Strategy and National Information Assurance Policy, drafting data-protection laws, and reaching out to Interpol to conduct a third-party review. The future will make such efforts even more important.

1. Smart Cities Highlight Necessity of Cybersecurity

Smart cities, for example, hold the promise of a higher standard of living for residents and business owners though the effective use of information and communications technology. Yet, security has to be built into the infrastructure because increasing connectivity can increase risk, said Mohammed Samiullah, Manager of IT Security and Domain Management for Msheireb.

"The more you are connected, the more vulnerable the attack surface becomes -- one vulnerability has the potential to become a catastrophe," he said. "That makes security a key element that we are looking at."

Qatar has made the development of smart cities a key initiative for the future, building new cities, such as Lusail and projects by Msheireb, from the ground up that will incorporate a variety of technologies to make citywide management and operations easier. QCERT is making the creation of cybersecurity standards for smart cities a priority in 2015.[45]

> **"Most smart city deployments in Qatar are planning on utilizing, and in some cases building local data center facilities to store the vast amount of user data collected by sensors and other smart services offered to residents and visitors. Access to this data will be strictly controlled to ensure user privacy, and at a minimum comply with the expected data privacy law, currently awaiting final government approval."**
>
> said Dr. Hosein Badran, Director of Special Projects at QCRI.

Cybersecurity is being built into the design of Lusail, with the central command-and-control systems using a private network, frequent design reviews and participation in attack assessments, said Ibrahim Kocagoz, Project Manager of Smart Cities for the Lusail City Development Project. "We are focused on protecting our infrastructure and our network from cyber attacks," he said. "We are considering all security aspects for which we are responsible."

As a whole, Qatar has taking measured steps to cybersecurity. This section describes some of the efforts currently underway in Qatar.

2. National Policies

The government of Qatar continues to develop a number of policies to advance cybersecurity, focusing on privacy, critical infrastructure and improving cybersecurity training and education.

Personal Information Privacy Protection Law

In 2011, the Qatari government published the first draft of its Personal Information Privacy Protection Law, which holds businesses and operators accountable for the personal information that they collect on citizens. The law has been approved by Qatar's cabinet and is now under review by the legislative committee.[46] The law sets guidelines for companies in protecting citizen data, especially that of children. Information deemed sensitive by the draft law includes geolocation data and information about sensitive topics, such as religious affiliations and medical conditions.

Guidelines and Legislation for Critical Infrastructure Protection

In February 2014, ictQatar released the second version of Qatar's National Information Assurance Policy, which gives companies a blueprint for creating effective security programs for critical industries.[47] While the Critical Information Infrastructure Protection Law is not yet in effect, it will require companies in the energy, finance, government, healthcare and telecom sectors to abide by regulations set by ictQatar.

A lab for testing critical infrastructure components is under development and Qatar will begin to use the Common Criteria, a set of standards for companies to attest to a certain level of security, said MICT's Sherin. "By 2018, those will be mandatory, and not just conditional," he said.

National Cyber Security Strategy

In May 2014, Qatar's National Cyber Security Committee released the National Cyber Security Strategy, a document that outlined five critical objectives for the nation to improve online and digital protections. The NCSS calls for efforts to safeguard critical infrastructure, speed response to incidents, share threat information, create an adequate legal framework, educate citizens and professionals in the safe use of cyberspace, and create a national cyber security capability. Improving cybersecurity is part of Qatar's efforts to create an advanced, robust information and communications technology (ICT) capability by 2015.[48]

Ongoing Cybersecurity Efforts

Interpol National Cybersecurity Review

Qatar is working with the newly established INTERPOL Global Complex for Innovation (IGCI)[49] to assess the nation's cybersecurity postures and capability to investigate and prosecute cybercrimes. The national cyber review collects and analyzes data on Qatar's capabilities highlighting strengths and weaknesses in cybercrime laws and enforcement.

> **"Right now, the cybersecurity risk facing all countries is high,"**
> **"But the fact that Qatar is pursuing this assessment highlights the significant resources and efforts they are investing into cyber."**
>
> said, Steve Honiss, from INTERPOL Global Complex for Innovation (IGCI).

3. Industry Efforts and Public-Private Partnerships

In addition to government efforts to create policy, legislation and regulations to improve cybersecurity, a number of initiatives bring together industry experts with public groups to better protect the information infrastructure.

Information Risk Experts Committees (IRECs)

Qatar has formed three public-private partnership groups to share information on threats and best practices in energy, finance, and government. Called the Information Risk Experts Committees (IRECs), the groups meet once a month, share anonymized incident information and collaborate on cybersecurity recommendations. While some countries, such as the United States, has more than a dozen such groups, Qatar requires far less, said MICT's Sherin.

"In some sectors, we only have one player in the industry," he said. "For so many years, for example, we only had only one telecommunications carrier. Now we have two."

STAR Cyber Exercises

To increase the readiness levels of both government and companies, Qatar's QCERT organized the second cybersecurity exercise, STAR-2, in December 2014. The exercise involved nine sector-specific scenarios to test response, improve teamwork, and increase awareness of cybersecurity issues within the nation's responder community. The exercise involved more than 320 participants from 30 large organizations from a variety of critical industries, including aviation, energy, finance, health, government and telecommunications.

Healthcare Security and Data Protection

By 2016, the majority of hospitals and some clinics in Qatar will be using electronic medical record systems. Yet, citizens and residents of Qatar may still have misgivings about whether their sensitive data will be protected and how it will be used. Because the most important stakeholder in healthcare is the patient, they need to know that they have privacy protections for their medical data, said Dr. Julio C. Silva, Chief Medical Informatics Officer at the Sidra Medical and Research Center.

"Part of it is to get them to feel comfortable and confident with their data being in these systems," he said. "We know that it is their data and we know that it is important."

While banking and financial services have fairly stringent security requirements, regulations in healthcare, energy and other sectors could be made more comprehensive, said Mostafa Essemmar, Manager of IT and Information Security at Sidra Medical and Research Center.

Healthcare and other sectors "could be more effectively regulated and benefit from standardized and specific security controls as the type of information and processes are very different from a sector to another," he said.

FIFA World Cup 2022

The preparations for the Fédération Internationale de Football Association (FIFA) World Cup in 2022 require that stakeholders within Qatar focus on cybersecurity. In 2014, the FIFA World Cup in Brazil became the target of significant cyber attacks. Hackers affiliated with the Anonymous movement conducted denial-of-service attacks against banks, government agencies and the FIFA organization. Attackers targeting Brazil vaulted the country to the top of the list of countries targeted by malware activity, with four times more attacks than those targeting second-place Russia.[50]

Qatar has already started speaking with other nations about their experiences in providing security for the World Cup games, both physically and online. In collaboration with Interpol, Qatari officials met with Brazilian authorities in November to discuss the lessons learned from the online attacks targeting Brazilian institutions.[51] In February, Qatari experts met with organizers from the United Kingdom, which hosted the 2012 Summer Olympics.

"As we approach the World Cup, the country is building new infrastructure, and it is all designed to be the latest in technology," said Omar Sherin of the Ministry of Information and Communications Technology. "This is our challenge: We are trying to learn from all previous experiences and lessons learned."

Contributors to the Report

Dr. Tamer Aboualy
CTO for Middle East and Africa, IBM Security

Mohammed Abu-Nejim
Head of Systems and Network Operations for Qatargas

Dmitri Alperovitch
Chief Technology Officer and Co-Founder, Crowdstrike

Omar Alrawi
Sr. Software Engineer, Cyber Security, Qatar Computing Research Institute

Shareef Ali Alsayed
Information Security Consultant, Ministry of Interior

Ali Majid Al Hashimi
IT Governance & Standards Manager, Information Technology Directorate, Qatar Foundation

Faisal Al Kuwari
Chief Technology Officer, Meeza.net

Dr. Mashael Al Sabah
Scientist, Cyber Security, Qatar Computing Research Institute

Dr. Hosein Badran
Director of Special Projects, Qatar Computing Research Institute

Mustapha Huneyd Bengali
Corporate Information Security in the Office of the CEO, Ooredoo

Cesar Cerrudo
Chief Technology Officer, IOActive

Dr. Marc Dacier
Principal Scientist, Cyber Security, Qatar Computing Research Institute

Dr. Soumitra Dutta
Dean and Professor of Management and Organizations, Johnson Graduate School of Management, Cornell University

Dr. Ahmed K. Elmagarmid
Executive Director, Qatar Computing Research Institute

Mostafa Essemmar
Manager of IT and Information Security, Sidra Medical and Research Center

Steve Honiss
National Cyber Review Manager, INTERPOL's Global Complex for Innovation

Osama Kamal
Cyber Threat Intelligence Section Manager, Qatar Ministry of Information and Communications Technology

Tom Kellermann
Chief Cybersecurity Officer, Trend Micro

Dr. Issa Khalil
Senior Scientist, Network Security and Secure Data Analytics, Qatar Computing Research Institute

Ibrahim Kocagoz
Project Manager of Smart Cities, Lusail City Development Project

Haroon Meer
Consultant for Al Jazeera/Founder and Principal Consultant, Thinkst

Jon Miller
Vice President of Strategy, Cylance

Ghareeb Saad Muhammad
Senior Security Researcher, Kaspersky Lab - Cairo

Dr. Ryan Riley
Assistant Professor, Department of Computer Science and Engineering, Qatar University

Dr. Guillaume Salha
Head Systems Engineer, Security Architecture, Qatar Petroleum

Mohammed Samiullah
Manager of IT Security and Domain Management, Msheireb

Dr. Dimitrios Serpanos
Principal Scientist, Cyber Security, Qatar Computing Research Institute

Omar Sherin
Critical Infrastructure Information Protection Department Manager, Ministry of Information and Communications Technology

Dr. Howard Shrobe
Principal Research Scientist, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology

Dr. Julio C. Silva, MD, MPH
Chief Medical Informatics Officer, Sidra Medical and Research Center

Dr. Jaideep Srivastava
Research Director, Social Computing, Qatar Computing Research Institute

Jen Weedon
Manager, FireEye

Dr. Ting Yu
Senior Scientist, Cyber Security, Qatar Computing Research Institute

Endnotes

1 ictQatar. National Information Assurance Policy v 2.0. Ministry of Information and Communications Technology. March 2014. PDF file.

2 Qatar Computing Research Institute. QCRI Emerging Cyber Threats 2014 Report. 26 Mar. 2014. PDF file.

3 General Secretariat for Development Planning. Qatar National Vision 2030. July 2008. PDF file.

4 INSEAD and Cornell University Johnson School of Business. The Global Information Technology Report 2014. World Economic Forum. 2014. PDF file.

5 Mia, Irene and Dutta, Soumitra. The Global Information Technology Report 2007-2008. World Economic Forum. PDF file.

6 Frost & Sullivan. Global Cyber Security Assessment 2014 - Executive Summary. 2014. PDF file.

7 Musil, Steven. Senate panel approves controversial cybersecurity bill. CNET News.com. 12 Mar. 2015. Web. 14 Mar. 2015.

8 Ministry of Information and Communications Technology (ictQatar). Qatar National Cyber Security Strategy. May 2014. 10-11, 14. PDF file.

9 Mackenzie, Heather. Shamoon Malware and SCADA Security — What are the Impacts? Tofino Security blog. 25 Oct. 2012. Web. 23 Feb 2015.

10 Cylance. Operation Cleaver Report. Dec. 2014. PDF file.

12 Cylance. Communication with author. Data not published in the Operation Cleaver Report.

13 Q-CERT. Fact Sheet: National Cyber Drill (STAR-2). ictQatar. 16 Dec. 2014. PDF file.

14 Lemos, Robert. "Cybersecurity information sharing initiatives on the rise." TechTarget. May 2012. Web.

15 Frost & Sullivan. Critical Times Demand Critical Skills: An analysis of the skills gap in information security. ISC2. 2013. PDF file.

16 Rassed Group and the Ministry of Information and Communications Technology (ictQatar). The attitudes of online users in the MENA region to Cybersafety, Security and Data Privacy. 2014. 42 - 43. PDF file.

17 Perlroth, Nicole. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back." The New York Times. 23 Oct 2012. Web.

18 See Cylance, Operation Cleaver.

19 See ictQatar, Qatar National Cyber Security Strategy, especially pages 10 and 13.

20 Ministry of Information and Communications Technology (ictQatar). Qatar National Information Assurance Policy (v2.0). March 2014. PDF file.

21 Greenwald, Glenn. How the NSA tampers with US-made internet routers. The Guardian: London. 12 May 2014. Web. 23 Feb. 2015.

22 Krebs, Brian. Target Hackers Broke in Via HVAC Company. KrebsOnSecurity.com. 5 Feb. 2014. Web. 23 Feb. 2015.

23 See Kaspersky Labs' Global Research & Analysis Team, The Desert Falcons.

24 See Cylance, Operation Cleaver.

25 SCADAHacker.com. n.d. Web. 14 Mar. 2015.

26 Dell Secureworks. 2015 Dell Security Annual Threat Report. April 2015. PDF. See pages 7 to 9.

27 Muhammad, Ghareeb Saad, Senior Security Researcher with the Global Research & Analysis Team at Kaspersky Lab. 22 Jan. 2015. Interview.

28 Bengali, Mustapha Huneyd. Personal interview. 28 Jan. 2015.

29 Spangler, Todd. Sony Pictures Targeted by Apparent Hack Attack to Corporate Systems. Variety. 24 Nov. 2014. Web. 10 Mar. 2015.

30 Muhammad, Ghareeb Saad, Global Research & Analysis Team at Kaspersky Lab. interview.

31 Kellermann, Tom. Personal interview. 19 Feb. 2015.

32 FireEye. Regional Advanced Threat Report - Europe, Middle East and Africa, 1H2014. Oct 2014. PDF.

33 See discussion in Kaspersky's The Desert Falcons targeted attacks.

34 Paganini, Pierluigi. "Syrian Electronic Army attacked most major Qatar websites." Security Affairs. 20 Oct 2013. Web.

35 Lemos, Robert. "Sony Pegs Initial Cyber-Attack Losses at $35 Million." eWEEK. 4 Feb 2015. Web.

36 Muhammad, Ghareeb Saad, Senior Security Researcher, Kaspersky Lab.

37 Correspondence with Shareef Ali Alsayed, Qatar Ministry of Interior.

38 Rassed Group and the Ministry of Information and Communications Technology. The attitudes of online users in the MENA region to Cybersafety, Security and Data Privacy. 2014. PDF file.

39 Rassed Group 28. Note: Survey is prior to revelations about mass surveillance by intelligence agencies via Snowden.

40 The Internet of Things. Cisco. n.d. Infographic.

41 Kramer, Adam et al. Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences of the United States. 17 June 2014. PDF file.

42 Schroepfer, Mike. Research at Facebook. Facebook newsroom. 2 Oct. 2014. Web. 15 March 2015.

43 Meer, Haroon et al. Weapons of Mass Distraction: Sock Puppetry for Fun & Profit." Oct 2014. PDF.

44 Qatar Foundation. Meeting Qatar's Grand Challenges. 21 Aug 2014. Web. 10 May 2015.

45 Interview with Omar Sherin, Ministry of Information and Communications Technology.

46 ictQatar. Ministry of Information and Communications Technology - Annual Report 2013/2014. 28 Jan 2015. PDF. Pg. 10.

47 ictQatar. National Information Assurance Policy v. 2.0. Feb 2014. PDF.

48 ictQatar. Qatar's National ICT Plan 2015: Advancing the Digital Agenda. July 2011. PDF.

49 INTERPOL. The INTERPOL Global Complex for Innovation. Web. 12 May 2015.

50 Kaspersky Lab. 2014 Cybercrime World Cup Brazil. 29 Jul 2014. Web. 5 May 2015.

51 Interpol. INTERPOL brings together sporting event security experts to exchange best practice. 24 Nov 2014. Web. 3 May 2015.

52 Aguilar, Joey. "Top Qatari official to meet UK cyber security experts." Gulf Times. 19 Feb 2015. Web. 12 May 2015.

Qatar Computing Research Institute
Tornado Tower, 18th floor - Doha, Qatar
Phone: +974 4454 0629 **Fax:** +974 4454 0630
www.qcri.qa

Qatar Computing Research Institute
Tornado Tower, 18th floor - Doha, Qatar
Phone: +974 4454 0629 **Fax:** +974 4454 0630
www.qcri.qa