<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the Executive Director</td>
</tr>
<tr>
<td>3</td>
<td>Introduction</td>
</tr>
<tr>
<td>5</td>
<td>Threat 1: Supply-Chain Security Weaknesses Invite Attacks</td>
</tr>
<tr>
<td>7</td>
<td>Threat 2: Attackers Target Critical Infrastructure to Disrupt Operations</td>
</tr>
<tr>
<td>9</td>
<td>Threat 3: Criminals and Advanced Attackers Target Mobile Devices and the Cloud</td>
</tr>
<tr>
<td>11</td>
<td>Threat 4: Information Manipulation and Media Threats</td>
</tr>
<tr>
<td>13</td>
<td>Threat Actors</td>
</tr>
<tr>
<td>14</td>
<td>Recommendations</td>
</tr>
<tr>
<td>16</td>
<td>Endnotes</td>
</tr>
</tbody>
</table>

**PREPARED BY:**

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

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

QATAR COMPUTING RESEARCH INSTITUTE
From online bank heists to industrial and nation-sponsored espionage, the threats that impact Internet-connected societies continue to evolve. Political and other differences readily manifest themselves online as Web site defacements and attacks on infrastructure and the media. Competition between companies and nations can lead to the infiltration of rival’s networks and the theft of data and state secrets. The Middle East and the Gulf Cooperation Council have become a stage where such attacks are frequently played out, sometimes from external actors but often by internal conflicts.

Static defenses against cybersecurity threats are not effective. Attackers continuously improve their techniques and technology, creating better attack tools and making their operations harder to detect and block. Qatar has directly felt the impact of these attacks: In October 2013, Syrian hacktivists used social engineering techniques to gain access to the Qatar Domain Registry and redirect nearly a dozen government and business Web sites to propaganda. Other nations in the region have suffered worse attacks. From the Stuxnet attack that destroyed Iran’s nuclear processing equipment to the Shamoon attack that deleted data on 30,000 computers at Saudi Aramco, the improvement in attackers’ tactics has a direct impact on businesses and governments in the Middle East.

To better understand the impact that such threats have on Qatar and its people, Qatar Computing Research Institute (QCRI) is pursuing a variety of research initiatives and collaborating with universities and research centers worldwide.

Continued on next page
QCRI was established in 2010 by Qatar Foundation for Education, Science and Community Development, a private, non-profit organization that is supporting Qatar’s transformation from a hydrocarbon-based economy to a knowledge-based economy. In support of Qatar Foundation’s mission, QCRI aims 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. The core values of QCRI include attaining the highest quality of scholarship, investigating innovative lines of research, fostering honest, ethical practices and collaboration among scientific peers, and leading discussions about scientific inquiry in academic, industry and local society.

In March 2013, QCRI hosted a roundtable to bring 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. On the anniversary of that roundtable, QCRI has created this report on the threats that impact Qatar and the region. The report brings together insights and analyses from a variety of experts from the IT security industry, government and academia both within Qatar and across the globe.

The report and the roundtable discussions are a starting point from which Qatar can foster an open discussion of emerging threats, their potential impacts on Qatar, and the development of defenses for containing them.

Sincerely,

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

In 2011, Qatar embarked on an ambitious plan to upgrade and expand its information and communications technology (ICT) infrastructure over the next five years as part of its planned transition from a hydrocarbon-based economy to an innovative, knowledge-based economy. Qatar’s National ICT Plan[1], due to be completed next year, encompasses five main strategic initiatives: improving connectivity, boosting capacity, fostering economic development, enhancing public service delivery and advancing social benefits.

While one strategic thrust, improving connectivity for all Qataris, focuses on increasing cyber safety and security, cybersecurity is a key component of the foundation of a modern, information-based society. Technology-dependent societies depend on safe and secure software, hardware and communications.

“Qatar is a very connected society with huge Internet penetration,” said Dr. Ahmed K. Elmagarmid, executive director, Qatar Computing Research Institute (QCRI). “More than 75 percent of phones are smartphones, digital government is pervasive, and people do most of their business online. Not paying attention to cybersecurity could jeopardize that.”

Yet, security is elusive in the technological age. Online criminals, espionage groups, cyber militias and political hackers—or hacktivists—directly threaten Qatar’s progress. A myriad of divides have been carried online, inspiring attacks, driving hostile groups together, and becoming the raison d’état for nation-state espionage. In October 2013, for example, hackers gained access to the domain-name registry accounts of nearly a dozen Qatari domains, redirecting visitors to propaganda sites.[2] In August 2012, Qatar’s natural-gas provider RasGas suffered widespread damage to its office systems when a virus deleted data from its desktop computers.[3]

Overall, cyber capabilities have grown quickly in the Middle East, and while some attacks have targeted Qatar, most activity has focused on other countries in the region. In the past, hacktivism has been a significant force—commonly used as a component of confrontations between opposing sides—but the use of the Stuxnet cyber weapon against Iran’s uranium enrichment capability demonstrated quite dramatically the potential of cyber operations.[4, 5] In addition, last year’s revelations of the capabilities of the U.S. National Security Agency (NSA), and the extent to which it collected data and monitored networks, raises questions about the security of all nations’ data and communications, not just from the NSA, but other major intelligence agencies as well.

Online activities, however, are not just driven by politics, but by financial gain. Cybercriminals operating from Eastern Europe, Asia and the Americas have developed sophisticated attack tools and processes to infect users’ computers and mobile devices to gain access to bank accounts and steal funds.

Qatar’s National ICT Plan

| improving connectivity | boosting capacity | fostering economic development | enhancing public service delivery | advancing social benefits |

Continued on next page
In December 2012 and February 2013, for example, a global hacking ring stole prepaid debit card numbers from Rakbank in the UAE and the BankMuscat in Oman, using the data to create fraudulent cards and rob ATMs worldwide of UAE Dh 165 million (QAR 163.5 million or U.S. $45 million). The primary hacking group, which remains at large, used low-level criminals in Britain, Canada, Columbia, Egypt, Japan, Romania, Russia, Sri Lanka and the United States to steal the money from ATMs.  

Such attacks and crimes underscore that defending against cyber attacks and cybercrime requires active participation by a variety of stakeholders. In addition, the general citizenry and the groups responsible for cybersecurity need to be aware of the threats to their infrastructure and data.  

“The attackers move quickly, so if your processes are getting in the way of defending the country, then you have to think seriously about how to improve your responses,” said Rich DeMillo, chief scientist at Qatar Computing Research Institute (QCRI).

Qatar’s progress will only continue to spotlight the country in the eyes of the world and as a leader in the Middle East. As the host of the 2022 Fédération Internationale de Football Association (FIFA) World Cup, Qatar will need to develop its cyber defenses to repel those who would want to disrupt the country’s infrastructure and stall its progress. With society increasingly doing business online, a disruption of the Internet and the computing infrastructure on which the country relies will cost Qatar and its people a great deal.  

To help inform the discussion of the nation’s cyber strategy, QCRI has created this report to describe the most significant emerging cyber threats and possible strategies to help the nation’s information economy be more resilient against them. Cybersecurity threats evolve quickly, and to be ready to defend against tomorrow’s threats, information technology professional and security researchers need to study what attacks may be just over the horizon. To continue on the path of prosperity, Qatar must develop its capabilities to detect, block and respond to threats before they impact the nation’s infrastructure, economy or populace. The threats have been organized starting with those affecting the most fundamental technologies, such as supplied software and hardware, to attacks on critical infrastructure to the more pervasive threats against mobile users and trusted content.
Supply-Chain Security Weaknesses Invite Attacks

Hacktivists focus on Internet infrastructure suppliers, while spies focus on hardware implants

The fast growth of infrastructure within Qatar, and the Gulf nations in general, makes the trustworthiness of the supply chain of primary importance. While suspicions of backdoor functionality commonly focus on networking hardware and software systems, the supply chain for most companies includes outsourced services and consultants who have privileged access to the networks and data of targeted companies. Increasingly, attackers are using these channels to compromise networks and data.

The most publicized example of attacks through the supply chain is the intelligence gathering techniques used by the U.S. National Security Agency (NSA). The intelligence documents leaked by former NSA contractor Edward Snowden detailed the wide variety of ways that a well-funded adversary could attempt to infiltrate a government or corporate network. While such techniques represent a danger, government agencies and companies should not ignore the more common attacks through third-party consultants and service providers.

“People are realizing that no system is absolutely secure, and security cannot be static,” said Srini Devadas, professor of electrical engineering and computer science at the Massachusetts Institute of Technology. “You need to both verify your supply chain, and then monitor for malicious traffic.”

DNS registries and registrars are a common point of attack

A common third-party vector of attack are providers of domain-name system (DNS) services, such as registries and registrars.

On October 18, 2013, ten government-linked Web sites—including the Ministry of the Interior, Ooredoo Qatar, and the Ministry of Foreign Affairs—began to display propaganda supporting the regime of Syrian President Bashar al-Assad. Attackers used a phishing attack—sending an e-mail that appeared to be official—to compromise an administrator at the Qatar Domain Registry, rerouting Web site requests for those ten domains to an attacker-controlled site. The result made it appear the sites were compromised, but in reality, the attack compromised the supplier’s management system.

The technique is not new. The Syrian Electronic Army appeared to hack the well-known U.S. newspaper, The New York Times, and a Web site belonging to the social media giant Twitter with a similar attack, fooling the companies’ providers, Melbourne IT, to change the site to which online visitors were sent. A similar social engineering attack fooled DNS registry Comodo, which issued certificates to an alleged Iranian nationalist, for major e-mail providers including Google Gmail, Yahoo Mail and Microsoft Hotmail; the certificates could have been used to make a fake site appear real, fooling the users of those e-mail systems.
Because DNS represents a fundamental technology on which the Internet relies, organizations should request greater security precautions, such as additional types of authentication and the ability to lock domains from changes.

Service providers can be a backdoor into company networks

As companies and government agencies shore up their networks against attacks, adversaries will aim to identify weaknesses in smaller, less secure companies. Attackers seeking to infiltrate the network of aerospace firm Lockheed-Martin, for example, focused on a smaller contractor. Cybercriminals successfully breached retail giant Target by compromising the company’s heating, ventilation and air conditioning (HVAC) contractor through which they gained access to Target’s network of payment terminals. Attackers seeking to infiltrate government or corporate networks using modified firmware embedded in a computer or network hardware, or a surveillance device embedded in anything from a USB cable to a power plug.[13]

Organizations should restrict third parties with privileged access to networks and data and limit service providers access to data. In addition, as contractors leave or service contracts expire, organizations should automate the deletion of privileges.

Compromised and counterfeit devices pose a threat

A year ago, supply-chain attacks on hardware and software systems were mainly a topic of research, with the occasional appearance of consumer devices infected with malware at the manufacturer. Yet, following the leak of intelligence documents by Edward Snowden, world governments have a much better concept of the possibilities for the compromise of devices in the supply chain. For example, a project codenamed “Ironchef” compromised the code in server motherboards giving persistent access to attackers, “Headwater” accomplished the same feat on Huawei routers, and “SurlySpawn” is a hardware implant that allows keystrokes to be gathered from a compromised keyboard by radar. The documents give a detailed picture of how a well-funded adversary could infiltrate government or corporate networks using modified firmware embedded in a computer or network hardware, or a surveillance device embedded in anything from a USB cable to a power plug.[13]

The United States is not alone in its intelligence gathering. China and Russia are both active in Middle East affairs, with Russia thought to be the more skilled adversary.[14] To combat the espionage tactics potentially used by such nations, a framework of standards is necessary to attest to the security of the supply chain.

“The supply chain is a big problem for all Middle Eastern countries, because it is very hard to check the integrity of supplied devices.”
— Ghareeb Saad, Senior Security Researcher, Kaspersky Lab

While the investigation of supply-chain attacks can cross into paranoia, both government agencies and corporate security teams should prepare themselves for the potential of compromised supply chains by regularly hunting down network anomalies, running incident response exercises and vetting suppliers’ own security measures.
While cybercrime has dominated the attack landscape in other parts of the globe, attacks on critical infrastructure—in particular, oil and gas processing and distribution systems—have grabbed the spotlight in Qatar and the Middle East. In the most noted attack, on August 15, 2012—while more than 55,000 employees were home preparing for Lailat al Qadr, or the Night of Power—an attacker logged into Saudi Aramco’s systems and unleashed a destructive virus known as Shamoon, which proceeded to infect three-quarters of office computers at the oil giant, deleting data on 30,000 PCs.

Less than two weeks later, another attack caused significant disruption at RasGas, a joint venture owned by Qatar Petroleum and ExxonMobil, temporarily cutting off e-mail and its Web sites from the Internet.

These attacks could have had a dramatic impact on the world economy. Because of the political environment and the intense rivalries between nations and non-state actors, cyber operations against critical infrastructure in the Middle East tend to be more destructive than in other similar incidents, with the possible exception of the destructive wiper attacks on South Korean firms, which mirrored the attacks on Saudi Aramco.

“In these cases, it is not just that the attackers want economic advantage, but they want the victims to struggle to recover,” said Dean De Beer, chief technology officer for ThreatGRID.

Distributed networks of embedded devices are difficult to defend

The monitoring devices and control systems used to manage critical infrastructure have become a popular target of security researchers and attackers. In one of the earliest known events, a disgruntled technician used stolen radio equipment to control the infrastructure installed by his former employer, leaking more than 800,000 liters of sewage into the surrounding rivers and parks of Maroochy Shire in Australia between February and April 2000.

In the 14 years since, distributed control systems have become more connected and, while vendors and critical infrastructure companies have begun to focus on security, the industry remains behind others, such as finance and software. Security researchers continue to find a variety of control system interfaces accessible from the Internet, such as the popular supervisory control and data acquisition (SCADA) protocol, while attackers are actively looking for such vulnerable systems.

“Many of the providers do not have proper zoning between the SCADA networks and their IT networks,” says Peter Baurichter, an information-security consultant based in Qatar. Part of the problem is that the two sides of business rarely collaborate, he said. “SCADA technicians typically don’t know that much about IT, and the IT people don’t know much about SCADA.”
The distributed nature of the systems make them difficult to manage and nearly impossible to update, without opening them up to further risk. While physical intrusions are a problem for any organization, the remote nature of many of the networks exacerbates the issue for critical infrastructure.

Researchers and attackers continue to focus on industrial control systems (ICS)

Security researchers and nation-state actors have shown attacks against industrial control systems are an effective way to disrupt critical infrastructure. In 2007, the U.S. government demonstrated an attack on a diesel-based electric generator—the Aurora Test Generator—damaging the equipment by hacking into the systems controlling the hardware. Two years later, the Stuxnet worm used similar techniques to damage and destroy centrifuges at the Natanz Fuel Enrichment Plant in Iran.

While security researchers had already begun looking at industrial control systems (ICS) and supervisory control and data analysis (SCADA) systems, interest exploded following the Stuxnet attack. For example, researchers discovered 25 SCADA software vulnerabilities and submitted them to the popular Zero Day Initiative bounty program in 2013, double the submission rate in 2012 and up from zero submissions in 2010. Because attackers frequently build on already pioneered research, such a stark increase in vulnerabilities reports should be worrisome, particularly because of the vulnerable configurations of many SCADA networks.

“Qatar understands that GDP may be hurt by incidents related to cyber security and the dangers that are increasing in the industrial control systems sector.”
— Dimitrios Serpanos, Principal Scientist, Qatar Computing Research Institute

While oil and gas infrastructure is most common target, other impacts could be significant

While the oil and gas industry is the most obvious target of cyber attackers, other industries should take steps to harden their infrastructure as well. Water processing, conducted under the management of the Qatar Electricity and Water Company, is another likely target of probes and attacks. While open-source intelligence on such attacks is not available, utilities in other nations have suffered similar attacks, and water utilities have been especially vulnerable.

“Qatar understands that GDP may be hurt by incidents related to cyber security and the dangers that are increasing in the industrial control systems sector,” Dimitrios Serpanos, principal scientist at QCRI, who leads its cybersecurity research team. “They are looking at improving from the organizational and technological point of view.”

Banks and financial systems in other Arab states have already been the targets of cybercrime as well. In the last 12 months, Arabic-language spam has increased dramatically, according to Russian security firm Kaspersky Lab. Such a surge likely indicates that attackers are increasing their interest in the region, so financial institutions need to harden defenses and educate consumers.
While much of the world is moving from desktop systems to smartphones and tablets, Qatar leads the world in its mobile usage, with each person owning an estimated 2.8 phones.\textsuperscript{[24]} The country leads a trend: By 2017, traffic from mobile devices used in the Middle East and Africa is expected to grow by 77 percent.\textsuperscript{[25]} With the proliferation of devices, many workers are increasingly bringing their own devices into the workplace and connecting to company networks. These two trends make Qatar attractive to cybercriminals focused on mobile-enabled crime.

Along with increases in mobile usage, especially smartphones and tablets, comes a dramatic increase in the amount of data stored in cloud services. More consumers are using Twitter and Facebook, storing their data in the cloud and communicating through cloud-accessible e-mail. These services, while their security capabilities may be better than the average company, represent a treasure trove for attackers, allow remote access to potentially sensitive data and could be subject to foreign regulations.

“People tend to rely more and more on these mobile devices for everything, from Internet access to cloud services to financial payments,” said Issa Khalil, senior scientist for Cybersecurity at Qatar Computing Research Institute (QCRI). “Unfortunately, there is not awareness of security, and that is a big problem.”

Criminals and Advanced Attackers Target Mobile Devices and the Cloud

As smartphones and tablets become the default way for users to get online and connect with each other, cybercriminals and spies focus on compromising the devices.

While Qatar has a far higher adoption rate of mobile devices than most other parts of the world, most users are generally not aware of security issues.

The prevalence of mobile use means that attackers will increasingly use phishing attacks and mobile malware to compromise users’ information.

The lack of a closed, secure ecosystem could result in higher levels of fraud and mobile-focused cybercrime.

The adoption of cloud services without adequate security education could result in breaches of business data and loss of private consumer data.

Attackers will focus on mobile because of widespread adoption.

Qatar’s lead in the adoption of mobile devices is an advantage as the country moves to a knowledge-based economy. However, financially motivated cybercriminals have already begun focusing on compromising mobile devices and conducting fraud campaigns against mobile users. Attacks on mobile users can occur in the Web domain, such as phishing and likejacking, or in the software domains, mainly mobile malware.

Because of its open platform and less stringent controls, the Android platform is the focus of 99 percent of malware attacks against mobile devices, according to security firms.\textsuperscript{[26]} While infection rates continue to be low, attackers are focusing on the development of mobile malware, the number of variants of which tripled in 2013, according to antivirus firms.\textsuperscript{[27]} Attacks such as Short Message Service (SMS) toll fraud are common, but using a mobile browser to phish login credentials from users is another common and potentially a more dangerous attack.

While Android is the most targeted operating system, any platform could be a victim of a targeted attack. Security researchers at the Georgia Institute of Technology in the United States, for example, have demonstrated multiple techniques for taking control of Apple’s popular iPhone.
Without a secure ecosystem, mobile malware will become a greater problem.

Modern mobile platforms have benefited from the security knowledge gathered by desktop software makers over the past three decades. Both Android and iOS systems have a number of security features that inhibit the execution of malware, alert the user to potentially hostile code, and check developers’ code for malicious functionality. Yet, such security measures require tight control by the mobile platform owners. The search for choice often leads users to remove a mobile device’s security that locks it to a particular carrier or service. Known as “jailbreaking,” the technique gives the user more control over their device, but also removes many of the security measures.

The lack of security awareness among mobile users, and the lack of security hints from devices, means that citizens will be more susceptible to fraud and attacks. “Mobile phones have not been a focus of security training,” said Yousef Khalidi, distinguished engineer at Microsoft. “We often don’t think of phones as something that can be hacked.”

As use of cloud services expand, data leakage and privacy threats will appear.

The adoption of cloud services is critical for businesses in a knowledge-based economy. Business becomes more efficient and agile with cloud services: Seven in ten companies that moved a business process to the cloud gained significant efficiencies and cost savings, according to global consulting firm KPMG. Yet, there are costs as well: A third of the companies found that implementation expenses were higher than expected and integrating cloud services with their company’s business processes took longer than expected.

In most cases, companies benefit from a cloud provider’s focus on security. Most cloud services can spend more and do a better job of securing their network than the average customer. Yet, putting data into a cloud service removes it from the hands-on control of the business and could put it in a foreign jurisdiction. Organizations should make sure that their business-sensitive data are not placed in cloud without adequate safeguards and controls.

“The cloud is a two-edged sword,” said Virgil D. Gligor, professor of electrical and computer engineering at Carnegie Mellon University. “Cloud companies can maintain their software better than the average person or company. But you have to trust the cloud administrators.”
The Internet and the broad acceptance of social media have, in general, benefitted society. When three Al Jazeera English journalists were arrested and held in Egypt on charges of spreading false news, protests on social media platforms spread worldwide, prompting governments to call for their release.[30]

Yet, the spread of information—especially false information—can be especially troubling. While social media became infamous for relaying information about popular uprisings in Egypt, Libya and Tunisia during the so-called “Arab Spring,” a great deal of false information was published and treated with equal credibility.[31]

“There are many types of organizations, both good and bad, that can and do use social media to their advantage,” said Irfan Essa, professor of computing with a focus on Computational Journalism at Georgia Institute of Technology. “It is not much different from the marketing machines in the West. It is really driven by using social media for persuasion tactics.”

As social media evolves, there will be a number of threats and challenges for Qatar and its neighbors in the Middle East.

Hacktivists and cyber militias continue to spread misinformation

In July 2012, the Syrian Electronic Army took control of the Twitter account of Al Jazeera’s English-language social media show, The Stream, posting statements supporting the Syrian regime.[32] Two months later, the group compromised Al Jazeera’s mobile news alert service, sending out a fraudulent message that claimed an attempt had been made to assassinate the Qatari prime minister. [33] And, in March 2013, the SEA hacked the Twitter and Facebook accounts of Qatar Foundation.[34]

“While it is questionable how much value the attackers gain from these tactics, they had significant impact even though the attacks were relatively unsophisticated,” said Haroon Meer, CEO and principal consultant for Thinkst, an information-security firm. “What is interesting is how much worse they could have been with a little bit more effort.”

The attacks demonstrate the attractiveness of online media to, not just legitimate users, but those who aim to spread misinformation and propaganda. Legitimate online protesters and other political dissenters have used a variety of tactics to get their voices virtually heard on the Internet. Yet, a number of governments have sponsored cyber militias to carry out their agendas online: the Syrian Electronic Army has supported the current regime, the Iz a-Din al-Qassam Cyber Fighters have been linked to Iran, and Russian cyber militias were implicated in the cyber attack on Estonia in 2007 and Georgia in 2009.[35]

The Internet is a powerful communications medium, but one that can be abused by outside forces. Qatar Computing Research Institute has begun to work on projects to look at the impact of such attacks.

Continued on next page
Denial-of-service attacks impact critical government and business services

In September 2012, the Iz a-Din al-Qassam Cyber Fighters began targeting primarily U.S.-based financial institutions with sophisticated distributed denial-of-service (DDoS) attacks. Such attacks typically attempt to overload networks or servers with a large number of requests. The DDoS attacks on banks, however, used a variety of tactics, including specialized requests designed to cause targeted servers to consume extra processing time.

Denial-of-service attacks, once thought to be a blunt tool used by unsophisticated hackers, have become a versatile and hard-to-block online threat. Used by cybercriminals, hacktivists and cyber militias the attacks can be used to censor a news site or blockade online services. In the recent past, the largest attack had peak bandwidths of hundreds of megabits per second; in 2013, the largest attack topped 300 gigabits per second.[34]

While such attacks have not been common in the Middle East, regional hacktivists have evolved their techniques to include the creation of botnets that could be used for massive distributed denial-of-service (DDoS) attacks. “We are increasingly seeing the spread of DDoS trojans through forums in the region as a way to create a large botnet,” said Ghareeb Saad, senior security researcher at Kaspersky Lab in Cairo. “We think that very soon we will start seeing massive attacks on government sites.”

Social networks can propagate unreliable information quickly

While the Internet allows people and companies to easily exchange ideas, those same low barriers for communications allow the rapid spread of unreliable stories. Chain e-mail threads, for example, have had incredible longevity, propagating a number of false ideas that echo throughout the Internet’s digital space. In some cases, these threads have been harmful.

With hundreds of television channels, innumerable Web sites, and the quick rise— and subsequent fall—of Twitter and Facebook pundits, using technology to determine whether information is reliable is a complex and extremely challenging task. In the end, the best solution will be for individuals to be informed and skeptical.

“The best filter for questionable content is an educated populace.”

— Yousef Khalidi, Distinguished Engineer, Microsoft
Currently, a variety of groups are operating in the Middle East. While some are obvious in their operations—such as the Syrian Electronic Army and the self-styled Cutting Sword of Justice—most groups do not advertise themselves and are only identified after the fact, if at all. Listed are descriptions of the potential adversaries affecting government agencies and companies in Qatar in order of the sophistication of their attack techniques.

True hacktivists are groups of technically-capable people brought together to support a single cause. Their most common methods are denial-of-service attacks to take down targeted networks, and Web site defacements, where a targeted Web site is replaced with the hacktivists’ message. Less common tactics include compromising targeted networks to steal customer data, business-sensitive intelligence or intellectual property, and then leaking it to the public. Hacktivism can bring together otherwise ideological incompatible groups in support of a single cause but typically does not last very long. The ideals of the Anonymous collective brought together a number of hacktivist groups to support pro-democracy protestors during the Arab Spring.[37]

Some apparent hacktivists have the funding or support of another organization or government. While such groups’ methods may resemble hacktivists, their message aligns with their sponsoring agency. In addition, such groups, typically known as “cyber militias,” tend to have much longer longevity than their hacktivist counterparts. Conflicts and rivalries between Middle Eastern states frequently have a cyber component that appears to be hacktivism, but serves the interests of their sponsors. Many nations—from China and Russia to Syria and Iran—have created or support hacking groups that serve their interests.[38]

A variety of nations have developed their capabilities to conduct operations in cyberspace. The most obvious example is the United States, which appears to have conducted extensive intelligence operations in the Middle East, and China, which has made information operations a national priority.[40] Russia is considered a more advanced and sophisticated adversary than China, with its operations rarely detected by security firms.[41] Following the Stuxnet attack on its uranium processing facility, Iran quickly developed its own cyber capabilities, creating the Supreme Council of Cyberspace and investing heavily to expand operations.[42] Israel has put enormous effort into maintaining a strong cyber capability as well.[43]
Recommendations

Much of the work needed to advance the state of cybersecurity in Qatar is fundamental, yet extremely difficult. While purchasing technology can help improve the nation’s cybersecurity posture, training people and gathering data on threats and defenses will have the largest ultimate impact.

“This is like dealing with cancer—there is no simple cure,” said Rich DeMillo, chief scientist of Qatar Computing Research Institute (QCRI). “You are never going to be able to eradicate the risk. Instead, you need a long-term program to reduce the risk to acceptable limits.”

Here are four recommendations that can significantly reduce the risk to Qatar’s information infrastructure and data.

**First Recommendation**

Gather data and share information

For any organization or government, the first step to defending against cyber attacks is to understand the problem and gain visibility into what is occurring within networks. Yet, roadblocks exist to gathering data and sharing information. Information sharing has been problematic in most regions, because companies are wary of sharing information with competitors and government request to businesses are rarely reciprocated, leaving companies in the dark as to what threats may be targeting them.[44]

Currently, there is a scarcity of data on cybercrime, malware infection and network probes in Qatar.

“Qatar is still adhering to the old model: Groups are not sharing the information,” said Omar Alrawi, senior software engineer for Cyber Security at Qatar Computing Research Institute (QCRI). “We need to have a community or working group that would be more open in terms of data sharing and joint projects.”

In other countries, many organizations have created industry-specific initiatives in conjunction with government stakeholders, such as the U.S. Financial Services Information Sharing and Analysis Center (FS-ISAC) and Japan’s Cyber Clean Center. Those types of organizations could be a way for local companies to gain defensive intelligence while protecting themselves from competitors. In addition, QCRI has a number of research initiative aimed at gathering data and gaining visibility into attackers’ techniques and targets.

**Second Recommendation**

Develop domestic security expertise and hacking culture

Technology alone cannot solve the problems. Instead, Qatar needs to focus on its most important assets: people. While creating defense in depth by implementing software patching, better monitoring of internal networks, and anomaly detection can harden networks and protect data, skilled security experts are needed to deploy and maintain the defenses.

Just as Qatar is developing a program to fund and train entrepreneurs, creating an environment where security experts—many of whom started as white-hat hackers—can thrive is important. Teaching security concepts at an early age can put some students on the right track. Taking part in cyber-defense competitions is another way to develop interest in computer and information security.

“There needs to be a focus on security education,” said Rich DeMillo, chief scientist of QCRI. “The security mindset has to reach down into schools, reach down into every aspect of the workforce.”

“**When the government and companies are working well together, infections rates go down. When there is unrest and public-private partnerships break down, infections go up.**”

— Tim Rains, Director of Trustworthy Computing, Microsoft
Third Recommendation

Educate workers and the general public about cybersecurity threats

While most people do not want to enter the information-security workforce, educating the general public, and especially knowledge workers, is equally important. People who are not trained to be aware of cybersecurity issues can inadvertently help attackers infiltrate networks.

“Whatever technology you are using, humans will be the weakest link,” said Issa Khail, senior scientist for Cybersecurity at QCRI. “So it doesn’t matter how many security measures you have, if the user is careless.”

While attackers look at people as victims to be fooled, every person can be a defender as well. Training people in basic information-security concepts can go a long way toward making the nation’s systems harder to compromise. For example, knowledge of the risks of supply-chain risks and education of employees can go a long way to mitigating the danger from supply-side attacks. While breaches are still most often reported by third parties, when they are detected internally, it is most often by employees recognizing suspicious activity.

Fourth Recommendation

Define responsibilities of stakeholders

The countries with the lowest number of infected computers in the world typically have close relations between the government and the private sector. Such public-private partnerships can lead to a lower incidence of malware, according to Microsoft, which has studied the socio-economic factors involved in malware infections. In the first quarter of 2011, 61.5 out of every 1,000 systems scanned in Qatar by Microsoft’s malware removal tool were found to be infected with the Rimecud worm. Yet, the Qatar Computer Emergency Response Team (Q-CERT) worked with companies to clean computers, bringing the infection rate to under 12 computers cleaned per 1,000 systems. The effectiveness of such efforts can be further enhanced with forward looking cyber security research, such as that conducted at QCRI to provide early warning of emerging threats to relevant stakeholders.

“Malware infection rates, in the cleanest countries in the world, are linked to public-private partnerships,” said Tim Rains, director of Trustworthy Computing at Microsoft. “When the government and companies are working well together, infections rates go down. When there is unrest and public-private partnerships break down, infections go up.”

Public agencies such as the Supreme Council of Information and Communication Technology (ictQATAR), the Ministry of Interior and organizations with an operational role like Q-CERT should work closely with private companies to create a more secure ecosystem. Qatar has already had its first National Cyber Security Drill (STAR-1). Such incident response exercises are both a necessary activity and can aid in clarifying the responsibilities. In addition, such exercises are an effective way to educate users and security workers on the proper response to threats.
Endnotes

Introduction


Threat 3: Criminals and Advanced Attackers Target Mobile Devices and the Cloud


[42] Harris, Shane, “Forget China: Iran’s Hackers are America’s New Cyber Threat,” Foreign Policy, 18 Feb 2014, http://complex.foreignpolicy.com/posts/2014/02/18/forget_china_iran_s_hackers_are_america_s_newest_cyber_threat


Recommendations


Contributors

Dmitri Alperovitch
CTO and Co-Originator, CrowdStrike

Omar Alraiwi
Sr. Software Engineer—Cyber Security, Qatar Computing Research Institute (QCRI)

Peter Baurichter
Information Security Consultant, Qatar

Dean De Meer
CTO, ThreatGrid

Rich DeMillo
Chief Scientist, Qatar Computing Research Institute (QCRI)

Sri Devadas
Professor—Electrical Engineering and Computer Science, Massachusetts Institute of Technology (MIT)

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

Irfan Essa
Professor in Computational Journalism, Georgia Institute of Technology

Brian Foster
CTO, Damballa

Virgil Gilgior
Professor, Department of Electrical and Computer Engineering, Carnegie Mellon University

Karl Gumtow
CEO of CyberPoint International LLC

Lance James
Head of Cyber Intelligence, Deloitte

Yousef Khalidi
Microsoft and a Qatar Computing Research Institute (QCRI) board member

Issa Khalil
Senior Scientist, Qatar Computing Research Institute (QCRI)

Haroon Meer
Founder, Thinkst

Tim Rains
Director and MENA Threat Expert, Microsoft

Sharea Saad
Senior Security Researcher, Kaspersky Lab—Cairo

Dimitrios Serpanos
Principal Scientist, Qatar Computing Research Institute (QCRI)

Lance Spitzner
Director—Securing The Human Security Awareness, SANS Institute

Ting Yu
Senior Scientist—Cyber Security Group, Qatar Computing Research Institute (QCRI)