ISSN 1941-6466

# Baker Institute Policy Report

Published by the James A. Baker III Institute for Public Policy of Rice University

NUMBER 53 SEPTEMBER 2012

## Cybersecurity Issues and Policy Options for the U.S. Energy Industry

### Introduction

On August 15, 2012, a representative of Saudi Aramco stated that Aramco "isolated all its electronic systems from outside access as an early precautionary measure that was taken following a sudden disruption that affected some of the sectors of its electronic network."[1] In the days that followed, news reports speculated that perhaps as many as 30,000 computers on the company's computer network were compromised by a malicious piece of software, possibly the one labeled *Shamoon* by the computer security malicious software ("malware") analysis community. Within days, a group calling itself the Cutting Sword of Justice declared that it was responsible for the Aramco disruption and that it would be redoubling its efforts against the company.[2] Meanwhile, large computer security companies, including Intel subsidiary McAfee and Russia's Kaspersky, began a process we have seen play out multiple times in the last few years: piecing together malware, target, attacker, and intent. The attack upon Aramco's network of computers, which still did not appear to be fully functional almost two weeks after the initial disclosure,[3] was yet another cyber incident to hit a major oil and gas company.

For more than a decade, a small community of computer security professionals and policy experts has debated the potential for malicious actors to subvert or compromise computer systems employed to manage the infrastructure of contemporary society: transportation, health care, water and sewage, telecommunications, and energy. While nightmare scenarios of cyberattacks probably appeared to be more science fiction than reality after low-tech hijackers in September 2001 launched the most successful terror attack against the United States in history, the record of network intrusions has grown with increasing rapidity. Though most incidents involve only purloining or corrupting data, at least one case—Stuxnet—apparently damaged physical machinery, as well. While defacing websites was once a viable tit-for-tat tactic of Internet hacktivist political expression, repeated breaches of energy company networks indicate that companies are now exposed to a significant set of cyberthreats.[4]

This report examines how energy companies, both those involved in the production and delivery of hydrocarbons, as well as those generating and transmitting electricity, are facing this new risk to the continuity of their operations, capacity to deliver products and services, and ability to protect investments—particularly in research and development—from theft or unauthorized disclosure. We consider two major areas in the energy industry susceptible to cyberthreats: (1) the vulnerability of its operations systems—the computers that route electricity, open valves, and operate motors—and (2) the problem of controlling access to proprietary corporate information and data, from internal email communications to long-term development plans and new technologies often carrying investments in the billions of dollars. After accepting that cybersecurity is an important issue in the energy industry, we must first address why cybersecurity legislation designed to protect the energy industry has not been met with approval in Congress, despite bipartisan backing.

### Legislation rejected

In the first days of August 2012, the U.S. Senate attempted to introduce new legislation designed, among other things, to improve the level of security for the networks of computer systems used by government, the private sector, and other public sector agencies. Interest in legislation on the topic of cybersecurity had grown significantly in Washington for several years. After a series of bills failed, a new piece of legislation, the Cyber Security Act of 2012 (CSA2012), was introduced in the Senate in July, following the issuance and passage to committee of earlier drafts across the span of the 112th Congress. Introduced by Sen. Joseph Lieberman (D-CT) and co-sponsored by four other senators, including Republican Susan Collins of Maine, CSA2012 was at root an effort to provide the federal government, through the Department of Homeland Security, a way to take on the perceived problem of an insecure cyber infrastructure—an infrastructure that is the pivotal component of almost all commercial, public health, and government activities in the United States.

Moved to the floor of the Senate for debate, the bill's sponsors were unable to assemble the 60 votes required to advance the legislation. A group of lawmakers, led by Sen. John McCain (R-AZ), argued against its passage. McCain stated, "There are those that believe any legislation is better than no legislation … I've been around long enough to know that isn't true."[5] McCain argued in favor of legislation he co-sponsored with Sen. Kay Bailey Hutchison (R-TX)—the SECURE IT Act, an effort to improve information sharing between government and industry on cybersecurity matters. Like earlier debates, cybersecurity legislation for 2012 was pushed back to 2013. The U.S. government had once again put off sweeping legislation that would have impacted industries across the country—including the energy industry, from oil and gas firms and services companies to electricity producers and distributors.

## What is the cyber problem for the energy industry?

For more than a decade, academics, policy wonks, and national security professionals have attempted to draw attention to the problem of computer networks being penetrated and controlled by unauthorized actors doing harm in various ways. The term "electronic Pearl Harbor," a massive surprise attack against the computer systems vital to the function of all manner of economic activity, remains a popular item of rhetoric. It is noteworthy how new the interconnection of computers to a global network—the Internet—is. Only 20 years ago, roughly one million computers and devices were connected to it; today, according to the Central Intelligence Agency, more than two billion people use it. In that brief period, it has become ingrained into almost every major economic endeavor of the United States and the developed world. As Shapiro and Varian observed more than a decade ago, information technology (IT) has stimulated revolutionary changes in some commercial activities and evolutionary ones in others, and has left some areas relatively untouched.[6]

IT is now heavily involved in the operations of energy production, processing, and distribution. Offshore drilling rigs, pipelines, refineries, power stations and, increasingly, distribution points for both fuels and electricity are becoming more and more interconnected by computer systems. The reason for unifying IT and embedding it across the energy supply and distribution chain is simple: Technology permits much greater awareness of operations, is a substantial aid to efficiency, and simplifies the underlying communication infrastructure. Beyond the computer systems that drive the infrastructure of energy production and distribution, there is another vitally important infrastructure that serves the *enterprise's* computing and messaging function for the employees of each energy company. These are the networks on which email is transmitted; plans are created, shared, and stored; and deals or trades are executed. For the geographically distributed petroleum firm, the capacity to communicate at a distance is a vital one.

The problem for this latter class of networks, however, is that there is a degree of risk associated with conducting digital activities and communications at a distance. For instance, storing digital materials like business plans or technical documents carries a degree of risk, because the ease of copying this material in a digital format is seamless, with essentially zero cost. Maintaining confidentiality and tight controls of digital information is an enormous problem without an easy solution. Two decades of massive investment in Internet-connected IT have produced significant productivity gains and efficiencies in the energy industry. However, those gains are now being offset by risks such as system compromises—by insider threats, competitors, and nation-states—that expose proprietary documents and processes. Additionally, there is growing concern that the systems that control processes throughout the energy supply chain are vulnerable to electronic tampering or manipulation. Discovery of the Stuxnet malware and revelation of its role in damaging centrifuges involved in the Iranian nuclear enrichment program stands as an indicator that the Rubicon has been crossed: computing systems can be subverted to produce physical results. This is a development with a profound impact on a number of industries that have come to depend upon computer control systems for operations—not least, the energy sector.

Understanding this particular vulnerability and what it means requires some background on how process control systems have developed and evolved. Addressing the security of those systems is a very small community of government, industry, and academic entities whose work is but a small niche in the rapidly growing area of information security. We begin our discussion with the substantive matters of concern in this area before moving onto the broader issues of information compromise.

## Security for process control

In the past few years, the security of supervisory control and data acquisition (SCADA) has risen to become one of the most important issues in information security. SCADA systems, or industrial control systems (ICS), are responsible for taking analog information from systems such as generator sensors or flow controllers and converting that information into a digital component so that it can be processed by an embedded system. A human or an automated or programmed function then acts upon the data, providing intervention when necessary. The importance of these systems is difficult to underscore, because without them much of the U.S. infrastructure would become unmanageable without massive human intervention. Process control automation has done to industry much what mechanization did to the agriculture sector: it has reduced the quantity of labor required to produce output.

Historically speaking, SCADA systems have generally consisted of several major components. At the highest level is the human-machine interface (HMI). HMI is anything that takes ICS information about a specific process and presents a sensor's reading to a human in an interpretable format. In addition to the HMI, there is a supervisory station, and this component is responsible for communicating with the remote terminal units (RTUs). RTUs are the communication endpoints that collect the data from programmable logic controllers (PLCs) and intelligent electronic devices (IEDs), which are sensors used to control or monitor the analog hardware (generators, pumps, or other machinery) that lie on the other side of the RTU.[7]

In the past, the priorities for developing and deploying successful SCADA systems have been data acquisition, accuracy, and reliability. These priorities are born out of engineering and safety requirements along with governmental regulation. An observer who is well-versed in the cyber domain is quick to point out that security is not part of this list. This exclusion is due in part to the fact that early ICS systems were isolated within the organization, so when these systems were put into operation, the thought of making them robust against the likes of espionage, sabotage, or terrorism was never really considered by the creators or the owners of systems. Essentially, the only security task necessary was to protect the components from direct unauthorized access, which could be accomplished by placing the components behind a literal lock and key.

After some time, these systems evolved into something that was more distributed. Rather than being monolithic mainframe systems in which all the sensors were physically connected to the same network, the SCADA RTUs, PLCs, and IEDs could be placed in remote regions, and the supervisory station could contact the sensor using a dial-up telephone modem. The distribution of these components is considered by most a step forward in the evolution of SCADA networks, and it is collectively referred to as the second generation.[8] Recall that the initial generation of SCADA systems relied on direct physical links. When direct physical links were not available, mediums such as a dial-up modem were used to communicate with the RTU. This meant the RTUs could be vulnerable to attempts to gain remote access via the telephone network, something known as "wardialing."[9] At this point of development in SCADA, information security was incredibly lax, meaning password protections were minimal, if present at all.

As SCADA systems evolved, they were increasingly interlinked, but not typically via Internet protocol (IP) networking. However, the latest evolution of these systems transitioned to this newer type of communication architecture. Specifically, the primary method of communication evolved from simply point-to-point (PPP) (e.g., just a modem) to connections over wide-area networks (WAN) via transmission control protocol/Internet protocol (TCP/IP). In some cases, PPP connections still existed, but the underlying communications packages were largely switched to TCP/IP. TCP/IP is the primary suite of communication protocols used by almost every computer globally to communicate with each other. This development of connecting inherently vulnerable SCADA systems to networks that are interoperable with Internet standard rendered their protection by obscure transport protocols obsolete. Since these sensors and service protocols may employ TCP/IP as the underlying communication standard, the challenge of successfully attacking SCADA systems is lowered due to the wide availability of network analysis tools for TCP/IP. Basically, SCADA went from a single, centralized supervisory system to a decentralized series of interconnected networks that was already vastly insecure. This interconnection has lowered the bar considerably for those who wish to communicate with and potentially compromise such systems.

As a countermeasure, energy firms have made investments in information security tools, processes, and education. In the traditional enterprise network, there is a set of information security practices applied to IT assets in an effort to protect them from internal and external threats. However, these principles were often not applied to ICS networks, either because they fell under the purview of the engineering department or because these systems, as mentioned previously, have very different requirements. This meant that a majority of the security stopped at the perimeter, resulting in a minimal set of protections for a very critical asset.[10] Additionally, given some of the intricacies of these applications and systems, SCADA and ICS systems security could also be further reduced due to misconfigurations or improper deployment standards. It should be also noted that even if common practices of IT were applied, these systems would still be very difficult to secure, given their proprietary nature or operational requirements. For instance, traffic from the RTUs may not be encryptable because the technical solution required, typically a "bump-in-the-wire" architecture, might introduce a timing delay that could prevent the supervisory controller from acting within the appropriate time window. Another example of a potential shortcoming in the traditional model is the allowance of third-party vendor access for technical support; this connection may not be necessary, but it is kept around in case there is an emergency.

## The SCADA security game changer: Stuxnet

With cyber defenses facing daunting prospects in mitigating the risk of security compromise, we should also consider how and why SCADA systems might be attacked. In general, attackers who actively target a SCADA system will be sophisticated; their goal will be very specific, and may include espionage, sabotage, theft, or potentially extortion. The very nature of a SCADA network makes it impractical for a typical minor actor, such as a cybercriminal gang or hacker activist group (e.g., Anonymous), to launch an attack. First, the people attacking these systems will need to understand how the various components and architectures work. In addition to understanding those concepts, they will likely require a deep understanding (e.g., ICS process map and controller-specific knowledge) of how to control parts of the system. The argument is not that the threat posed by a traditional attacker is low, but rather that the objectives and capabilities of the attacker are likely to be incredibly limited. For instance, an attacker unfamiliar with a particular SCADA system could send a number of malformed packets to the supervisory station and consequently send the incorrect commands onto an RTU, which might result in a failure somewhere in the process. Under most circumstances, such an attack will likely alert a human operator, and human intervention can be used to circumvent or reduce any consequential damage from the event. However, as demonstrated by a widely publicized video of an exercise undertaken by the U.S. Department of Energy's Idaho National Lab, the results can cause immeasurable loss. In the video, an attacker has managed to gain some type of access and manipulate a generator in a physical plant, which ultimately ends with the generator's failure.[11]

Under more subversive circumstances, an attacker who is attempting to cross over into an organization's SCADA network will more likely have a more specific objective in mind. This inclination appears to have been exactly the situation in what is likely the first acknowledged case of an international cyberoperation designed to impact physical infrastructure: Stuxnet.

Stuxnet is regarded as one of the most sophisticated, publicly-known cyberattacks to date. It should send a clear message that most critical infrastructure is vulnerable to cyberattack. In some circles, the parties argue that Stuxnet demonstrated nothing more than a well-funded attack that was designed and developed by one or more nation-states targeting another nation.[12] It has far-reaching implications for global Internet governance; the position of the United States on cybersecurity policymaking; and, perhaps most importantly, demonstrates that what was once hypothetical is now in fact real and can be done.

Stuxnet differs from many of the other attacks that have been observed in the past because it accomplished many things with a relatively compact piece of software code.[13] It targeted an air-gapped infrastructure and rewrote PLC code aimed specifically at the Siemens SCADA systems employed in Iran's Natanz nuclear facility. After some very intricate investigative work, Ralph Langer[14] was able to reverse engineer the Stuxnet code and attribute specific elements of the code to images that were posted on Iranian websites. Furthermore, he was able to piece together how the software intentionally sabotaged the uranium enrichment process. Symantec also provided insight into the way Stuxnet navigated the IT infrastructure through the infection of network shares and detachable media such as USB flash drives. Overall, Stuxnet exploited seven vulnerabilities, but four of the exploits took advantage of four previously unknown vulnerabilities.[15] Furthermore, Stuxnet utilized a peer-to-peer system that allowed it to spread through the network and propagate updates along with other information.

No doubt, Stuxnet was a sophisticated cyberattack, but what does it mean for commercial organizations' SCADA and ICS networks? In short, it means organizations need to rethink their cybersecurity in both the strategic and tactical sense. Until recently, there has been very little public documentation that an organization could reference to help build its IT security posture, let alone judge its effectiveness, highlighting the need for more actionable information and policy. Currently, there are a number of documents about information security, with only a few of them touching on SCADA. One problem with a majority of the documents in this limited pool is that they cover too much information for an already overtaxed security professional to evaluate and use to improve infrastructure, let alone to build effective security organizations capable of dealing with threats. The National Institute of Standards and Technology (NIST) Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*,[16] and North American Electric Reliability Corporation (NERC) *Reliability Standards for Critical Infrastructure Protection*[17] are two examples of elaborate technical documents that cover the strategic and tactical security in SCADA networks. The Department of Energy has also released two documents: *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*,[18] which focuses on how to build the IT security organization and evaluate success; and the *Cybersecurity Risk Management Process (RMP) Guideline*,[19] which is based on NIST Special Publication 800-82. The Idaho National Labs also has training on SCADA security with materials posted online for owners who maintain these types of systems. These online materials can help provide a quick overview and training to help identify and mitigate vulnerabilities in a SCADA network.[20] However, it should be noted that exploring these materials requires a professional who is both fluent in security and who understands the needs of his or her organization. But, above all, understanding and applying these concepts requires time and buy-in by *all* stakeholders in the energy sector.

## Intellectual property and cyberespionage

Gen. Keith Alexander, director of the National Security Agency and head of the U.S. Department of Defense's Cyber Command, believes that cyberespionage accounts for the "greatest transfer of wealth in history," with U.S. companies losing about $250 billion from theft and another $114 billion from incident clean-up (e.g., digital forensics, notifications, investment in further security, etc.).[21] Those firms that have been targeted rarely acknowledge reports of cyberindustrial espionage publicly. On January 12, 2010, Google took a decidedly different approach when it released a blog post stating that it was the target of both political and industrial espionage, and attributed the attack to computer systems in China.[22] After Google went public, other prominent IT firms, including Juniper, Rackspace, and Adobe, also made public statements regarding attacks related to those observed by Google. More details on this set of espionage activities came to light after the independent hacker organization Anonymous compromised security consulting firm HB Gary Federal and released internal emails stolen from the company. Through these mails, the impact of what was labeled by the IT industry as "Operation Aurora" reached across hundreds, if not thousands, of organizations.[23]

Evidence that concerted attempts have been made to compromise technologies designed to maintain the confidentiality of enterprise information resources is troubling.

In 2011, a successful attack was launched against RSA, a prominent information security firm[24] offering authentication software and systems for enterprise networks. Attackers specifically targeted RSA to gain access to cryptographic information used to derive pseudo-random numbers employed by one of RSA's core products, SecurID.[25] The SecurID system is used to perform two-factor authentication, especially when users are connecting to the internal network from a remote location, like a hotel room or home. Once the attackers had access to this information, they were then able to perform follow-on attacks against military contractors, including Lockheed Martin and L-3 Communications. Specifically, the attackers were able to use the cryptographic material to authenticate with the contractors' remote access systems, commonly known as virtual private networks (VPNs). In the case of Lockheed, the attack was initially successful, but the overall operation was stopped due to a rapid internal response.[26] The impacts of the L-3 attack were never publically discussed. Another contractor, Northrop Grumman,[27] disabled all remote access services and reset all internal user accounts. This example highlights how sensitive intellectual property stolen from a vendor was used to successfully attack third-party clients, and these responses should also highlight how serious the contractors perceived the threat to be. Fortunately, these companies were able to anticipate the attack and had some way to respond to the threat when it materialized.

In another series of cyberattacks, dubbed "Night Dragon" by McAfee, the company that discovered them, Chinese attackers actively targeted global energy companies.[28] The end result of these attacks was the massive exfiltration of documents related to internal project estimates, bids, and emails, in addition to other sensitive documents.[29] The attacks were instigated primarily through the exploitation of external services like web servers and spear phishing. (Spear phishing is discussed in detail on page 7.) Once the attackers had access to an energy company's internal network, they would upload access tools that enabled them to control machines remotely and sift through the network looking for high-value content. Once the high-value content was identified, the information was then exfiltrated out of the organization's network.

In other high-profile cases, the perpetrators of the corporate espionage have actually been employees or contractors, and these individuals used their network privileges to gain access to copious amounts of proprietary information. In one case, a Motorola employee, Hanjuan Jin, was apprehended as she was preparing to abscond to China.[30] When she was taken into custody, she was found to be carrying a significant quantity of Motorola intellectual property and trade secrets protected by U.S. law. She had also been concurrently working for a competitor, Lemko, while she was employed with Motorola.[31] Jin was convicted of theft of trade secrets in February 2012.[32] In another case, a DuPont employee was convicted of trade secret theft. Before leaving his position with the company, the employee downloaded over 20,000 documents and viewed as many as 16,000 more.

But the Jin case and others like it represent what may be becoming an entirely outmoded method of industrial espionage. Placement of covert operatives, while potentially quite rewarding, is also dangerous and can produce significant blowback. We need look no further than the U.S. government's gross vulnerability—demonstrated by the alleged leaking of diplomatic cables to the WikiLeaks website by an enlisted intelligence specialist—to show how a trusted insider may damage an institution's capacity for maintaining confidentiality. There is also a considerable capacity for harm without placing an individual inside a targeted organization through means such as spear phishing attacks or computer network exploitation. If awareness can be established inside the enterprise network of a major corporation, there may be immense rewards in piecing together the intentions of that firm and working to purloin from its intended plans and technologies. This is largely because of the enormous production and distribution of digital content (e.g., email), which allows instantaneous communication at global distances.

Most organizations deliver Internet-based services to their employees via two basic conduits—access to online content via Internet browsers and email—and both are problematic. Email scales well to so many devices and locations because it is fundamentally simple; however, as any email system manager will attest, email addresses are an open door for those wishing to communicate from outside the corporation to addressees within it. For example, when an email address is mated to an individual unique address, it is oftentimes based on the person's actual name. Social networking sites further exacerbate this issue, because it increases the ease of cyberstalking and identifying co-workers and their current or past roles within the organization. What follows is a simple conduit for delivering malicious software that can eavesdrop on specific users of that address and also self-propagate across the internal network to other users' computers and devices—a form of malware known as a worm.

What has developed into the cyberespionage tool of choice over the last few years is a delivery of emails that appear to be authentic and to come from a trusted source. This tactic is referred to in information security circles as spear phishing. Spear phishing attacks use a purposefully crafted email aimed at a specific individual or set of individuals. The spear phishing email usually contains an attachment with a clandestine software payload designed to eavesdrop on the recipient, copy itself to other computers and servers, and, ideally, not be discovered by the targeted individual or organization. The party launching the spear phishing attack does not need to be anywhere within the organization's IT infrastructure; it only needs to hold valid email addresses for individuals inside the organization, preferably those with a high degree of access to sensitive information. To make the most impact, initial intelligence is valuable in producing a message subject, content, and attachment that is believable. A hacking group or intelligence service targets an organization, creates a malicious email, and sends the spear phish email to the organization.[33] This is the general pattern that has been associated with intrusions designed to purloin intellectual products and internal communications of foreign firms by Chinese actors.[34]

If and when the email is opened, the exploit code contained in the attachment or the message is executed. Once the executable is unpacked and running, it simply calls back to a command and control (C2) server or servers using an unsuspicious route—for instance, the hypertext transfer protocol (HTTP).[35] Such protocols are employed in cyberespionage because they are the universal services through which most organizations allow both inbound and outbound traffic. The C2 servers can be any server, either wholly owned by the adversary or another organization's asset, that has been compromised.

Once the backdoor software is installed and running, it will call out to the C2 machines periodically. As was observed in the case of the Chinese adversarial teams, HTML comments can be embedded in the web pages that a Trojan horse—another type of malware—polls.[36] When the attackers want access to the network, they send commands to the program, which downloads a backdoor and starts the program. When the backdoor is run, it connects to a server of the attacker's choosing and provides remote access to the network.

The clandestine eavesdropping enabled by successful spear phishing attacks permits the massive exfiltration of data from the organizational network to unauthorized parties. While remote eavesdropping no doubt varies in efficacy and duration, the key issue for organizations wishing to maintain some semblance of secrecy is to detect the activity as rapidly as possible and to expunge their computers and network of the offending malware. Neither task is trivial, nor are technical means for detecting intrusions entirely effective. Off-the-shelf security products largely defend against known malware and perhaps have the capacity to compare commonality with other known pieces of malware. Until a piece of system-compromising software becomes known and flagged, it has the potential to pass along confidential information to unauthorized parties. Understanding this vulnerability is not simply a technical function, as computer security research has often been surpassed by innovation in systems-compromise software and tactics. Furthermore, this threat is not simply limited to social engineering tactics like spear phishing. Since cybersecurity issues in the energy sector have attracted attention, products used to combat cyberattacks are being analyzed and egregious flaws are being exposed publicly because no other venue exists to get them fixed—which was the case with the recent exposure of RuggedCom devices.[37] When critical vulnerabilities percolate into the public eye, even the most vigilant energy company is kept from absolutely securing its networks. For players in the energy sector, a more realistic approach to cyberthreats may be found in risk models that consider broader geopolitical and economic figures in understanding what entities and individuals may be targeted in each company, and even the industry at large.

## The geopolitics of cybersecurity and energy

In March 2007, the Baker Institute, in partnership with the Japan Petroleum Energy Center, conducted a sweeping study on the changing role of national oil companies (NOCs) in the face of growing global demand for oil and gas.[38] The papers produced for the project outlined how national economic development and international political goals are often interwoven. When it comes to cybersecurity and the energy industry, it is important to consider the set of actors that represent potential threats of disruption and damage to systems and infrastructure—and the theft of information held dear—but in electronic form.

Anecdotal evidence is now substantial with respect to incidents in which the confidentiality of corporate information has been violated. Generally, there is now an increasingly well-understood assumption that with regard to cyberespionage, it is no longer *if* a company will be hacked, but rather *when*. This is because the intelligence services of nation-states have increasingly shifted to cyber means to collect intelligence. No doubt the world's major powers, the United States included, are developing significant cyberintelligence collection capacities as an outgrowth of their existing signals intelligence activities. The pivotal question is this: to what degree are national intelligence services supporting the economic activities of corporations in their deal-making and acquisition of technology?

China is a frequent target of official accusations from the United States regarding espionage, as evidenced by the creation of the U.S.-China Economic and Security Review Commission (USCC), established at the behest of the U.S. Congress in 2000. The commission holds as its mandate, "To monitor, investigate, and submit to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, to Congress for legislative and administrative action." In recent years these reports have been replete with expressions of concern regarding China's cyber capabilities, both in espionage and potential military application. In 2009, the USCC contracted with Northrop Grumman, a defense firm with major IT and cybersecurity portfolios, to study the issue of cyberconflict with China.[39] The report chronicled the vast literature created by Chinese military academicians regarding the potential to exploit information technologies to nullify the military advantages of China's adversaries.

While much has been written about China, cyberwarfare, and the problem of deterrence in the cyber domain,[40] less considered is Chinese cyberespionage directed at advancing the interests of the nation's industries and economic well-being. From the hacking of the Dalai Lama's computer network to the repeated compromise of Falun Gong activists' email accounts, a nervous and insecure China—preoccupied by internal dissent in what remains a nondemocratic, one-party state—comes into relief. A national firewall ostensibly protects the citizenry from threatening or seditious ideas, although many within the country appear able to manage end runs around it. Accusations of Chinese cyberespionage recur with great frequency and are backed by verifiable cases of espionage against U.S. firms and interests.

With regard to China, the great unknown is to what degree the different intelligence organs of the People's Liberation Army (PLA) and other pieces of its government engage in cyberintelligence collection and analysis to further the interests of China's NOCs—chiefly, China National Petroleum Corporation (PetroChina); China Petrochemical Corporation (Sinopec); and China National Offshore Oil Corporation (CNOOC). Similarly, there is the question of what Russian oil and gas firms receive from the successor intelligence agencies of the Soviet Union. With Russia, however, it is fairly easy to draw a straight line from its intelligence services to key posts in its energy sector. Standing as an exemplar is Igor Sechin, a likely one-time main intelligence directorate (GRU) agent once posted to Angola and now chief executive officer of petroleum firm Rosneft, as well as deputy prime minister in Russian President Vladimir Putin's cabinet.[41]

But casting the intelligence activities of Russia and China in a naively sinister light does little to help the current state of affairs in cybersecurity for the energy industry. Traditional U.S. allies are also willing to engage in economic espionage as well, with France's Direction Générale de la Sécurité Extérieure (DGSE), the country's foreign intelligence service, widely reputed to engage in espionage aimed at aiding French firms. One such case may be a bungled break-in of China Eastern Airlines chief Shaoyong Liu's Toulouse hotel room in December 2010.[42] In addition, NOCs have been targeted by cyberespionage activities. The Flame malware cyberespionage tool was reputedly found at Iran's Kharg Island oil terminal. Even more recently, reports emerged of cyberespionage software being discovered on the computer network of Saudi Aramco.

This all illustrates that in contemporary economic espionage, a two-way street likely exists and standing on moral high ground is but the weakest of arguments upon which to castigate the Russians or Chinese. Because it is at best difficult and in many cases virtually impossible to attribute cyberespionage to a specific entity, there is little to lose in engaging in the behavior, especially if it may be undertaken under the banner of state interest. Private firms operating in the oil and gas sector should recognize this reality and reconsider how to confront the problem. To what degree cyberespionage is a concern for public policy in the United States, among its allies, and globally is the final issue explored in this report.

## Policy prescriptions for cyber-risk in the energy sector

The widespread deployment of the Internet began just 20 years ago, yet it has fundamentally transformed business operations in multiple economic sectors. Information technology serves as a fundamental input for corporations operating globally in the business of energy, from hydrocarbon exploration to final-mile electricity delivery. Computing is a fundamental component of business operations, from relatively unsophisticated upstream and downstream system monitoring sensors to peta-flop scale supercomputers employed in exploration, research, and development. Removing IT from energy production and distribution is as tenable an option as asking the board members of any U.S. corporation to leave their cell phones at home, something that many of the agencies in the U.S. Intelligence Community expect of their employees every day. The energy sector, much like transportation, logistics, entertainment, and medicine, is in the process of a digital transformation with an unclear end state. Thus, establishing what can be done today may have little utility in informing laws or rules intended to be enforced for decades.

We opened this report with a discussion of the 2012 cyber bill, which like its predecessors will now be relegated to legislative history and likely retooled for Congress' next session. Cybersecurity advocates—including United States Association for Computational Mechanics chairman Eugene Spafford, Center for Strategic International Studies' James Lewis, and former White House cybersecurity special adviser Richard Clarke, as well as the Joint Chiefs of Staff and a number of firms in both the defense and IT sectors—supported the 2012 bill, but it failed to come to a vote. Opponents of the bill, led by the U.S. Chamber of Commerce, made the argument that the proposed legislation was nothing more than regulation and that, "Regulations are not a panacea and, in fact, could make improving cybersecurity more difficult."

Important lessons on what regulation means in cybersecurity can be taken from the U.S. federal government's own cybersecurity regulations, which were most recently amended by the 2002 Federal Information Security Management Act (FISMA). Passed with bipartisan support and requiring action from federal agencies, the National Institute for Standards and Technology, and the Office of Management and Budget, FISMA was designed to make uniform the processes by which the unclassified computing systems of federal agencies and those firms that provide services to the federal government under contract are secured against compromise by unauthorized parties.

The linchpin of FISMA is the certification and accreditation (C&A) process. This is an attestation of due diligence that a system is validated for operation without compromise; until such a validation is made, no system shall be placed into active use. Unfortunately, the FISMA C&A process has received justifiable criticism that it is more an exercise in paperwork than a concerted effort to monitor and harden information systems.[43] NASA's information security director balked at what he viewed as FISMA's burdensome reporting requirements and opted instead for a program of continuous monitoring. The paper process of C&A probably improved systems security to some degree by remedying the low-hanging fruit in systems security, such as applying necessary system patches and other updates as well as putting into place items probably most accurately described as best practices.

FISMA's fundamental flaw is likely that it attempted to emplace structures by which cybersecurity risk would be diminished while not itself being dynamic enough to provide a remedy for advancing threats and new adoption of technologies throughout the U.S. government. Worse, it only covers unclassified computer systems, which are typically the only ones with full, if monitored, contact to the Internet. FISMA was placed into law when Facebook's Mark Zuckerberg was still a student at Harvard, Wikipedia had fewer than 10,000 articles, and Twitter did not exist. The 2012 cyber bill called for significant amendments to FISMA, but it is unclear how those changes would have altered the implementation process across the U.S. government.

So with FISMA a less than ideal template for legislation, we must ask what can be done in the arena of public policy, especially considering the unrelenting rate of change in the IT sector. There are probably two answers, one very much local and organic, and the other global. The first is embodied by a hope that universal concern among firms in the energy sector will lead to sector-specific cooperation, coordination, and investment. The largest players in oil and gas likely have the budgetary capacity to purchase almost every security device, appliance, and service available on the open market, as well as retain highly qualified personnel and develop internal technologies and practices. But herein lies the rub. Those firms transact with service companies, specialists, law firms, and other actors in the course of business. An important question for super-major oil and gas chief information officers is, to what degree are their partners up to par in securing their systems?

In traditional realist approaches to the security dilemma, that of war and peace, states have formed bonds of mutual cooperation aimed at extending deterrence. Belgium, the recurring speed bump in the wars of conquest undertaken by Europe's great powers, has enjoyed almost seven decades of uninhibited territorial sovereignty, due in some part to the collective security provided by NATO's capacity to deter aggression. But NATO's members are countries, not companies. Energy firms compete aggressively to secure reserves, develop capacity, and expand market share. But in aggregate, how shall they behave when facing competition from state-owned firms that may be able to significantly damage their capacity to produce revenue and maintain technical superiority? The West's oil and gas companies arguably remain capable of producing results with capital and labor resources that have yet to be equaled by state-run firms. Mexico, with its rusty Pemex infrastructure, stands as an exemplar of the limitations of state-run petroleum companies.

There is an argument to be made that through the theft of information, NOCs may strengthen their capacity to do business without the investment and cooperation of firms that remain independent of government. While this may represent an extreme, cybersecurity prognostication is full of imaginative leaps in which mass technology subversion leaves modern society in the cold and dark. Cybersecurity may not represent an existential threat to U.S. firms or companies in the energy sector, but it does appear a more real threat than perhaps five or 10 years ago. Energy still has two major concerns to accept: the capacity of competitors, principally the intelligence proxies of NOCs, to see inside their organizations; and the problem of mitigating the vulnerability of process control systems as they become interlinked and networked. Several suggestions may be valid.

1. Recognize the example of Google. It was undeterred by its own security breaches and sought an asymmetric remedy to its issues with China (i.e., advocacy for Internet freedom there and temporary withdrawal from the Chinese market). While wholesale public disclosure is probably not an option, wider cooperation among firms already working collaboratively on projects regarding security issues is a must. Development of overarching security practices and protocols for joint efforts should be considered a prerequisite for such activities.
2. Consider the value of trusted third parties. They may collect and pool cyberattack data, especially regarding unique threats in a research context. The energy industry participates in the InfraGuard and ICS-CERT; however, it should consider how to deepen collaboration on discrete technical matters, such as malware analysis and unlocking the root logic of spear phishing and establishing advanced countermeasures against it. Similar activity is already underway regarding cybersecurity in the financial sector.
3. Take what information is offered. The energy industry should position itself to receive cyberintelligence from U.S. government agencies and those of allies when that information is timely and relevant. The reporting and analysis of the National Security Agency, the Department of Homeland Security, the FBI, and the constituent elements of U.S. Cyber Command should be available to energy companies and provided in declassified digests whenever practicably possible.
4. Foster the development of models for cyber-risk intelligence. Energy firms need to combine their abundant geopolitical and economic knowledge with inputs from their IT organizations to understand not just the "what and when" in the event that their information systems are attacked, but also the "how and why." Consideration should also be given to methods for information fusion regarding cyber issues.
5. Assess the costs. Wherever possible, the same sort of analytical rigor regarding production, processing, and delivery costs should also be applied to the IT space so that efficacy of security efforts may be more accurately assessed and economies may be located.
6. Finally, be paranoid. While international ventures in critical cyberthreat countries may be worth the financial risk, cyber policies should scale to those venues,

and practices should be emplaced that compartmentalize and shield information of greatest value to the enterprise.

To accomplish these goals, nothing in the way of new laws or regulations is needed to pass through Congress, although funding for the public components of public-private partnerships and additional programmatic initiatives will obviously require congressional approval. Nonetheless, there are practical, organic activities that may be undertaken inside and outside of the United States to likely build on lessons already learned and programs already underway. The energy industry is known for accepting significant risk and managing it. By working as a community it may reduce its cybersecurity vulnerabilities, serve as a model for other industries, and avoid burdensome and costly regulation of potentially dubious value.

## Conclusion

Energy firms have spent vast sums on the security of their information systems, but they must reorient from a reactive, tactical posture regarding intrusions and attacks to a more strategic, holistic view that expands beyond the categorization of the issue as only an IT problem. For the energy industry, cybersecurity is not just a technology problem, but rather is one that includes the larger dynamics of information and operations. How public policy can form components of the response to cybersecurity issues pertaining to the energy industry and the critical infrastructure that it builds, operates, and maintains requires considering both the complexity of the issue and the nuance in potential policy prescriptions.

The set of studies undertaken by the Baker Institute in 2007 expressed concern regarding the possibility of independent oil companies (IOCs) being shut out of production opportunities by NOCs and the governments to which they report. In the five years since the NOC study—a dramatic change in energy supply, enabled by technological innovations that unlocked the oil and gas found in shale—has altered the geopolitical calculus of energy. While this technological innovation has occurred principally in the United States, the grand concern is that the innovation surrounding shale and other novel energy technologies will be purloined via cyber means and brought to market by foreign competitors with state backing.

While the authors are cognizant that the technologies themselves are only a component of the innovation in the energy sector, as people and processes certainly matter as well, the amount of know-how that could be collected through a compromise of corporate internal communications, principally via email, should be of concern. Beyond this, there is the problem of protecting technological innovation—which extends beyond those who develop it to those employing it, and even to legal experts and law firms responsible for protecting intellectual property by patent.

In the oil and gas industry, IOCs face competition from national competitors and are exposed to significant geopolitical risk due to the political instability found in many of the core production areas around the world. While a reminder of the so-called "oil curse" is important—with major exporters often failing to shift oil revenue to projects and programs that improve general well-being in their countries[44]—these countries do not yet appear able to perform the sorts of network penetration and cyberespionage activities performed by China and Russia. What is difficult to measure is how much impact Gen. Alexander's "greatest transfer of wealth" has on the energy sector. This is a matter that IOCs should seek to better understand and quantify.

Moving beyond cyber espionage, there is the looming threat to networked control system infrastructure. As SCADA has been integrated with TCP/IP, the potential for a real cyberattack capable of physically impacting electricity generation and transmission as well as upstream and downstream oil and gas operations has moved from hypothetical to possible. Those who might choose to engage in such acts may well include not only the proxies of NOCs, but also potentially aggressive states, terror organizations, and politically motivated hacker groups, exemplified by Anonymous. How this set of threats may develop is fairly easy to imagine.

Organizations with the capacity to collect large quantities of information regarding process control systems architecture and develop highly customized software code able to subvert those systems are few on the planet today and are likely only found in the governments of nation-states. Knowledge about cyberattacks against infrastructure may proliferate because functions found in sophisticated malware such a Stuxnet may be redesigned and repurposed for other attacks. Controlling the proliferation of cyberattack software is very difficult once that software has propagated across the Internet. There is no reason to believe that attacks of the nature of Stuxnet will not eventually arise outside the world's most sophisticated state-run offensive cyber organizations.

The issues of cyberespionage and true cyberattacks—the ability to achieve kinetic outcomes by manipulation of computer systems—represent significant challenges for the energy industry, the United States government, and the international community. Establishing institutions to cope with these problems and move beyond a reactive posture will require greater research investment, collaboration, and unorthodox combinations of expertise from within the computing field and beyond it.

## Endnotes

1. "Saudi Aramco Responds to Network Disruption," Saudi Aramco, accessed August 26, 2012, http://www.saudiaramco.com/en/home.html#news%257C%252Fen%252Fhome%252Fnews%252Flatest-news%252F2012%252Fsaudi-aramco-responds-to-network-disruption.baseajax.html.

2. Kelly Jackson Higgins, "Shamoon, Saudi Aramco, and Targeted Destruction," *Dark Reading*, August 22, 2012.

3. Daniel Fineren and Amena Bakr, "Saudi Aramco says most damage from computer attack fixed," *Reuters*, August 27, 2012.

4. Mark Clayton, "U.S. oil industry hit by cyberattacks: Was China involved?" *Christian Science Monitor*, January 25, 2010.

5. Ramsey Cox and Jennifer Martinez, "Cybersecurity Act fails Senate vote," *The Hill, Hillicon Valley: The Hill's Technology Blog*, August 2, 2012, http://thehill.com/blogs/hillicon-valley/technology/241851-cybersecurity-act-fails-to-advance-in-senate.

6. Carl Shapiro and Hal Varian, *Information Rules, A Strategic Guide to the Information Economy* (Cambridge, Mass: Harvard Business Review Press, 1998).

7. Tobias Walk, "Cyber-attack protection for pipeline SCADA systems," *Pipelines International Digest* (January 2012): 5-8, http://www.ilf.com/fileadmin/user_upload/publikationen/Pipelines-International_Jan12_Cyber-attack-protection-for-pipeline-SCADA-systems_Walk.pdf. See also: Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke, "SCADA security in the light of Cyber-Warfare," *Computers & Security* 31 (June 2012): 418-436, accessed August 16, 2012, doi:10.1016/j.cose.2012.02.009.

8. Tobias Walk, "Cyber-attack protection for pipeline SCADA systems," *Pipelines International Digest* (January 2012): 5-8, accessed August 16, 2012, http://www.ilf.com/fileadmin/user_upload/publikationen/Pipelines-International_Jan12_Cyber-attack-protection-for-pipeline-SCADA-systems_Walk.pdf.

9. Wardialing is an automated process of calling phone numbers in an effort to discover modems. In general, the person performing this activity is trying to identify unprotected or weakly protected systems. Essentially, once an attacker discovers a system, he can attempt to probe it even further. If a system is password protected, the attacker can perform a dictionary attack, where he attempts to guess the password from a dictionary of words, or he can attempt a brute force password attack, where he tries to exhaust all possible combinations of characters that can be used to create the passwords.

10. Traditionally, these are firewalls, router access control lists (ACL), and intrusion detection and prevention systems (IPS/IDS). Firewalls and router ACLs help block traffic before it has an opportunity to enter and exit the network, but these safety measures are limited because they can only statically block traffic based on Internet addresses and ports; in some cases, the communication protocol is not static, and they cannot block traffic based on content (e.g., the data contained in the network communication). The IPS/IDS systems can use a variety of techniques to examine traffic content and even a specific protocol's behavior, but these systems tend to be very noisy with respect to false positive events, and if an attack is previously unknown, then these systems are likely to miss the attack.

11. Bruce Schneier considered the development through his blog, *Schneier on Security*, in 2007, summarizing of SCADA that, “the risk is overblown today but is getting more serious all the time—and we need to deal with the security before it's too late.” Bruce Schneier, *Schneier on Security*, http://www.schneier.com/blog/archives/2007/10/staged_attack_c.html.

12. Gregg Keizer, “Is Stuxnet the 'best' malware ever?” *Computerworld*, September 16, 2010, accessed August 16, 2012, http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_.

13. Nicolas Falliere, Liam O Murchu, and Eric Chien, “W32.Stuxnet Dossier,” Symantec Security Response. February 2011, accessed August 16, 2012, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

14. Ralph Langer, “S4 Stuxnet Attack Code Deep Dive,” SCADA Security Scientific Symposium - S4, accessed August 16, 2012, http://www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/.

15. The vulnerabilities exploited are:

i. Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability,

ii. Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability,

iii. Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability,

iv. Windows Escalate Task Scheduler XML Privilege Escalation,

v. Microsoft Windows Kernel 'Win32k.sys' Keyboard Layout Local Privilege Escalation,

vi. WinCC hardcoded credentials, and

vii. Overwriting protected functions in what should be execute only memory on the PLCs.

16. Keith Stouffer, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems (ICS) Security*, (special publication 800-82, U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, NIST, 2012), accessed August 16, 2012, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

17. “Critical Infrastructure Protection Standards,” North American Electronic Reliability Corporation, December 16, 2009, accessed August 16, 2012, http://www.nerc.com/page.php?cid=2%7C20.

18. “Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),” Department of Energy, accessed August 16, 2012, http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012.

19. “Cybersecurity Risk Management Process (RMP) Guideline - Final (May 2012),” Department of Energy, accessed August 16, 2012, http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

20. “National SCADA Test Bed Program: Intermediate SCADA Security Training,” Department of Energy, accessed August 16, 2012, http://www.inl.gov/scada/training/d/8hr_intermediate_handson_hstb.pdf.

21. Josh Rogin, “NSA Chief: Cybercrime constitutes the ‘greatest transfer of wealth in history,’” *Foreign Policy*, July 9, 2012, http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

22. David Drummond, “A new approach to China,” *Google Official Blog*, January 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

23. Michael J. Gross, “Enter the Cyber-dragon,” *Vanity Fair*, September 1, 2011, accessed August 16, 2012, http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109.

24. The company’s name is derived from co-founders Ron Rivest, Adi Shamir, and Len Adleman, inventors of the public key encryption algorithm, which bears their last initials.

25. Gross, “Enter the Cyber-dragon.”

26. Tom A. Peter, “How bad was the cyber attack on Lockheed Martin?,” *Christian Science Monitor*, May 29, 2011.

27. Gross, “Enter the Cyber-dragon.”

28. “Global Energy Cyberattacks: ‘Night Dragon,’” McAfee, accessed August 16, 2012, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

29. Mark Clayton, “U.S. oil industry hit by cyberattacks: Was China involved?” *Christian Science Monitor* (2010).

30. Andrew Harris, “Ex-Motorola Worker On Trial For Stealing Secrets For China,” *Bloomberg*, November 7, 2011, accessed August 20, 2012.

31. Lou Kilzer, “Motorola, spinoff settle suit involving China,” *Tribune-Review*, February 1, 2012, accessed August 16, 2012, http://triblive.com/x/pittsburghtrib/business/s_779346.html.

32. Jim Carr, “Sentencing in DuPont insider theft case delayed again; former scientist faces 10 years in jail,” *SC Magazine*, accessed August 23, 2012, http://www.scmagazine.com/sentencing-in-dupont-insider-theft-case-delayed-again-former-scientist-faces-10-years-in-jail/article/35203/.

33. Such attacks extend beyond organizational email addresses, with Google detecting attacks on the personal email addresses of U.S. government officials, journalists, and others, on its Gmail email service. Google fingered the physical source of the spear phishing attacks against Gmail to Internet addresses in Jinan, China. Eric Grosse, “Ensuring your information is safe online,” *Google Official Blog*, June 1, 2011, http://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html.

34. Michael Riley and Dune Lawrence, “Hackers Linked To China’s Army Seen From EU To D.C.,” *Bloomberg*, July 7, 2012, accessed August 16, 2012, http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html.

35. Adam Pridgen and Matthew Wollenweber, “Intelligence Report: Analysis of a Spear Phishing Attack,” *Hackin9 Magazine*, February 1, 2010, accessed August 16, 2012, http://thecoverofnight.com/paper/pridgen_wollenweber_phishing.pdf.

36. Michael Riley and Dune Lawrence, “Hackers Linked To China’s Army Seen From EU To D.C.,” *Bloomberg*, July 7, 2012, accessed August 16, 2012, http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html.

37. RuggedCom devices were found to contain secret key information making it possible to compromise any and all devices made by the Siemens subsidiary. Dan Goodin, “Private crypto key in mission-critical hardware menaces electric grids,” *Ars Technica* (2012), http://arstechnica.com/security/2012/08/mission-critical-hardware-flaw/.

38. *Baker Institute Policy Report, No. 35, The Changing Role of National Oil Companies in International Energy Markets* (Houston: Baker Institute for Public Policy, April 2007).

39. Bryan Krekel, “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” (prepared for The U.S.-China Economic and Security Review Commission, October 9, 2011), http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

40. Chris Bronk, “Blown to Bits: China’s War in Cyberspace, August–September 2020,” *Strategic Studies Quarterly*, Spring 2011.

41. Heidi Brown, “Igor Sechin: The Kremlin’s Oil Man,” *Forbes*, November 11, 2009.

42. Toulouse serves as headquarters for European aircraft manufacturer Airbus, which operates major manufacturing facilities in France; Germany; Spain; the UK; and, since 2009, Tianjin, China. Jean Guisnel, “La DGSE prise la main dans le sac à Toulouse,” Le Point.fr, January 21, 2011, accessed August 20, 2012, http://www.lepoint.fr/chroniqueurs-du-point/jean-guisnel/la-dgse-prise-la-main-dans-le-sac-a-toulouse-21-01-2011-130875_53.php.

43. W.A. Conklin, “Why FISMA falls short: The need for security metrics” (proceedings of the Second Annual Workshop on Information Security and Privacy - WISP 2007, [SIGSEC pre-ICIS], Montreal, Canada, December 2007).

44. Mahmoud El-Gamal and Amy Myers Jaffe, *Oil, Dollars, Debt, and Crises: The Global Curse of Black Gold* (Cambridge: Cambridge University Press, 2009).

All article links may be found in the digital version of this report at www.bakerinstitute.org/policyreport53.

Rice University's
Baker Institute – MS40
P.O. Box 1892
Houston, Texas 77251-1892

## Acknowledgments

The authors would like to thank Deloitte LLP for its support in the research activity from which this paper was drawn. The principal author of this report is Christopher Bronk, Ph.D., fellow in information technology policy at Rice University's Baker Institute. Adam Pridgen, the secondary author, is a graduate student and cybersecurity researcher in the Department of Computer Science at Rice University.