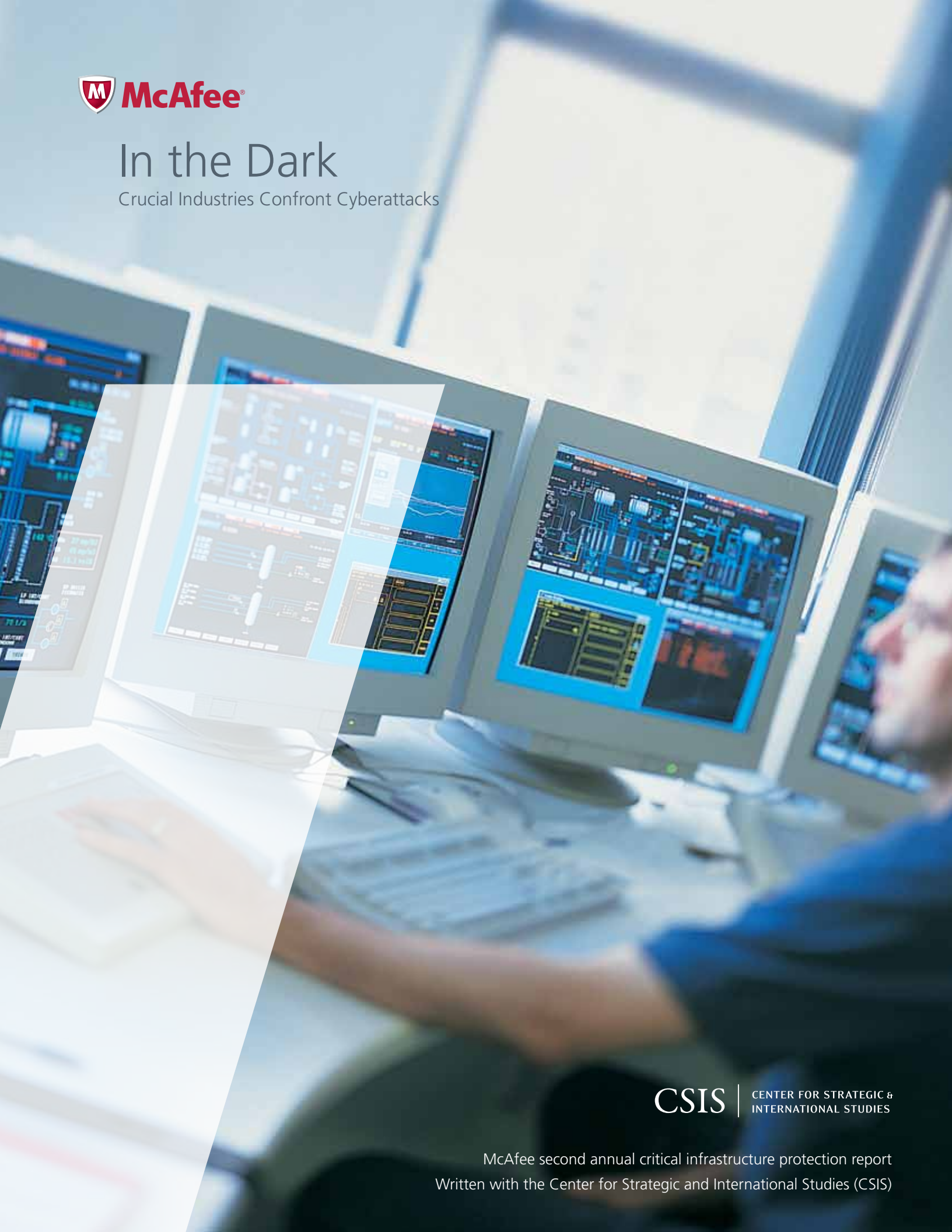
McAfee

In the Dark

Crucial Industries Confront Cyberattacks



CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

McAfee second annual critical infrastructure protection report

Written with the Center for Strategic and International Studies (CSIS)

In the Dark

Authors:

Stewart Baker, distinguished visiting fellow at CSIS and a partner at Steptoe & Johnson law firm

Natalia Filipiak, program manager and research associate at CSIS

Katrina Timlin, research assistant at CSIS

CONTENTS

Introduction and Summary

A year ago, the McAfee report, "In the Crossfire: Critical Infrastructure in the Age of Cyberwar," showed just how vulnerable critical infrastructure around the world is to cyberattack. In the year since that report, Stuxnet has transformed the threat landscape. It was a sophisticated, successful, weapon with a single purpose—sabotaging an industrial control system.[1]

This year, in a sequel report, we focused on the critical civilian infrastructure that depends most heavily on industrial control systems. As with the first report, we used survey data, research, and interviews to obtain a detailed picture of cyber risks in these sectors. The sectors on which this report focuses—power, oil, gas, and water—may well be the first targets for a serious cyberattack.

What we found is that they are not ready. The professionals charged with protecting these systems report that the threat has accelerated—but the response has not. Cyberexploits and attacks are already widespread. Whether it is cybercriminals engaged in theft or extortion, or foreign governments preparing sophisticated exploits like Stuxnet, cyberattackers have targeted critical infrastructure.

Many of these threats pose harsh new challenges for the industries' IT professionals. Today, "If you can't deal with a zero-day attack coming from a thumb drive," says former Director of Central Intelligence Jim Woolsey, "you have nothing."

We found accelerating threats and vulnerabilities. For the second year in a row, IT executives in the critical infrastructure sector told us that they perceive a real and growing cyberthreat. Denial-of-service attacks on energy networks increased. Extortion attempts were also more frequent in the CIP sectors. And hostile government infiltration of their networks achieved staggering levels of success.

Vulnerabilities are also still growing. Forty percent of executives believed that their industry's vulnerability had grown over the past year—outnumbering by almost two to one the executives who thought it had decreased. Between one fifth and a third of all respondents told us that their company was not at all prepared, or not very prepared, for cyberattacks ranging from malware to denial-of-service—a figure that has not improved much since last year.

Despite these vulnerabilities, many power companies are doubling down on the danger; they are implementing "smart grid" technologies that give their IT systems more control over the delivery of power to individual customers—or even to individual appliances in customers' homes. Without better security, this increased control can fall into the hands of criminals or "hacktivists," giving them the ability to modify billing information and perhaps even control which customers or appliances get electricity. But security is not a priority for smart grid designers; according to Woolsey, who two years ago chaired a group that published a report for the Department of Defense on grid vulnerabilities. "Ninety to ninety-five percent of the people working on the smart grid are not concerned about security and only see it as a last box they have to check."

There have been only modest improvements in security

Last year, we tried to measure security objectively, asking specific questions about companies' use of 29 particular security technologies, from encryption to authentication. We used their responses to create an objective scale for exactly how many security measures companies were putting in place. Gauged objectively, industry executives made modest progress over the past year in securing their networks—adopting about half of the security technologies we identified. The energy sector increased its adoption of security technologies by a single percentage point, to 51 percent, while oil and gas executives reported an increase of 3 percentage points, to 48 percent. The only notable increase was in water and sewage, a sector that lagged last year but that increased adoption of security measures this year by 8 percentage points, to 46 percent.

Almost exactly the same pattern held true when we asked about adoption of security measures for respondents' Industrial Control (ICS) or Supervisory Control and Data Acquisitions (SCADA) systems. While better network security is not simply a matter of throwing more and more technology at the problem, increased adoption of particular technologies does offer objective evidence that companies are not just talking about increased security. They are doing something—but only a little more than they were doing last year.

There is much room for improvement. Sixty percent of the IT executives we interviewed report that they required tokens or smart cards for offsite users to log on to critical systems, as opposed to the easily hacked user name and password, and more sophisticated measures, such as tools to monitor network activity or detect role anomalies, had been adopted by a minority (25 percent and 36 percent, respectively) of the respondents.

Threat Perceptions and Responses Varied by Country

Looked at by country, the above-mentioned gaps in security are even more striking, with laggard countries like Brazil, France, and Mexico having adopted only half as many security measures as leaders like China, Italy, and Japan.

The differences also persisted in terms of threat perceptions. For example, 90 percent of Australian respondents believed their respective sectors were not at all or not very prepared for stealthy infiltration attacks. Along the same lines, three out of four Brazilian respondents and six out of 10 Mexican respondents felt their companies were unprepared for a large-scale distributed denial-of-service (DDoS) attack. Another outlier in the report was India, where nine out of 10 executives said they expected a major cyberattack within a year.

Government's Role Is Still Unclear

How are governments responding to the vulnerability of their core civilian infrastructures? In general, they continue to play an ambiguous role in cybersecurity—sometimes helping the private sector, sometimes ignoring it.

Here, China continues to draw the most attention. China's government seems to play an aggressive role in demanding security from its critical infrastructure. Chinese government security requirements, for example, are viewed with respect by Chinese respondents, and China had the second highest rate (after Japan) of government security audits. In contrast, companies in the United States and United Kingdom almost never experienced government security audits.

This pattern also partially corresponded to confidence levels that respondents had in the ability of current laws to prevent or deter attacks in their countries: the highest levels of confidence were found in Japan (78 percent), the United Arab Emirates (UAE) (67 percent), and China (56 percent). If there is a race among governments to harden their civilian infrastructure against cyberattack, these responses suggest, Europe and the United States are falling behind Asia.

Globally, industries fear attacks by governments, and more than half of respondents say that they have already suffered from government attacks. What has changed since last year is the country that looms largest in such fears.

"Ninety to ninety-five percent of the people working on the smart grid are not concerned about security and only see it as a last box they have to check."

–Jim Woolsey, former United States Director of Central Intelligence.

Last year, the United States and China were neck and neck as countries of concern, with the United States somewhat more prominent. This year, though, China stands alone, while the United States has dropped to third place.

Roughly the same percentage of respondents (30 percent) still cite China as a major source of concern for cyberattack. What has changed is that China now stands alone as the country of greatest concern, followed more distantly by a group of countries that includes Russia, (16 percent), the United States (12 percent), North Korea (11 percent) and India (4 percent). The decline of the United States (from 36 percent last year) as a source of concern, and the relative rise of other countries, may be due to a realization by IT executives in the sector that cyberattack technology has begun to proliferate widely.

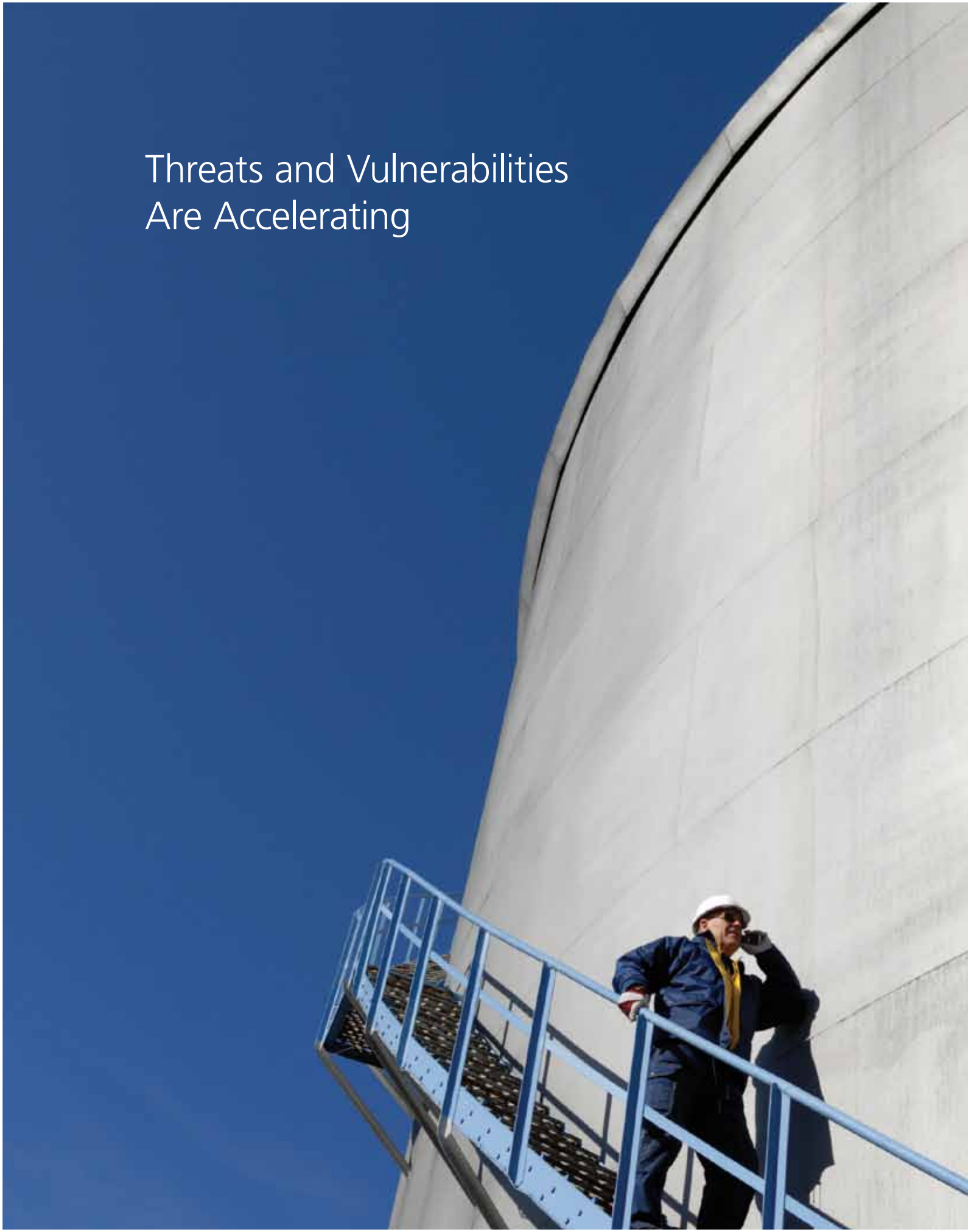
Methodology

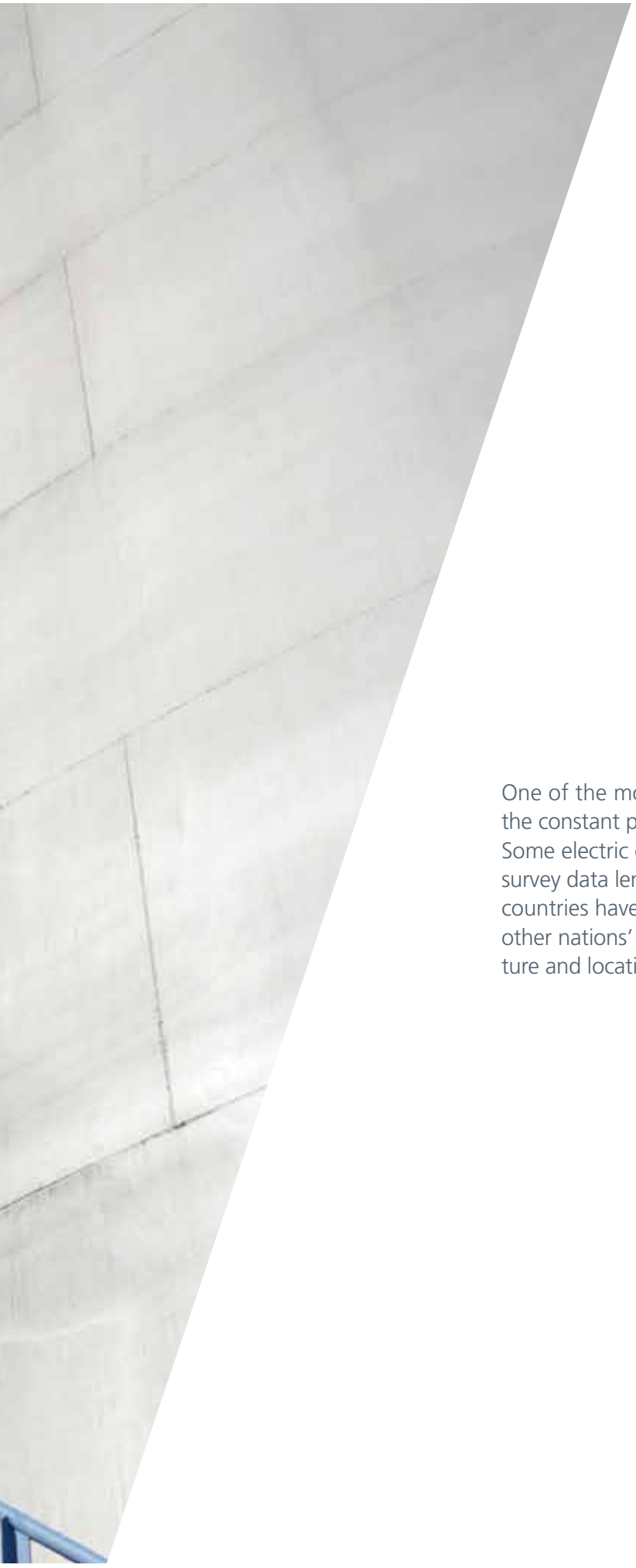
We surveyed 200 industry executives from critical electricity infrastructure enterprises in 14 countries, who anonymously answered an extensive series of detailed questions about their practices, attitudes, and policies on security. The respondents were drawn from a pool of IT executives in the energy, oil/gas, and water sectors. Their primary areas of responsibility were information technology security, general security, and industrial control systems. A team from the Center for Strategic and International Studies (CSIS) in Washington, DC analyzed the data, supplementing it with additional research and interviews.

The survey measures executive opinion, providing a snapshot of the views of a significant group of decision-makers in critical infrastructure sectors. The CSIS team also used interviews to provide context, background, and verification for the survey data—adding detail to the picture of the electricity grid and the threat/vulnerability levels of this utility sector and discussing best practices.

Globally, industries fear attacks by governments, and more than half of respondents say that they have already suffered from government attacks.

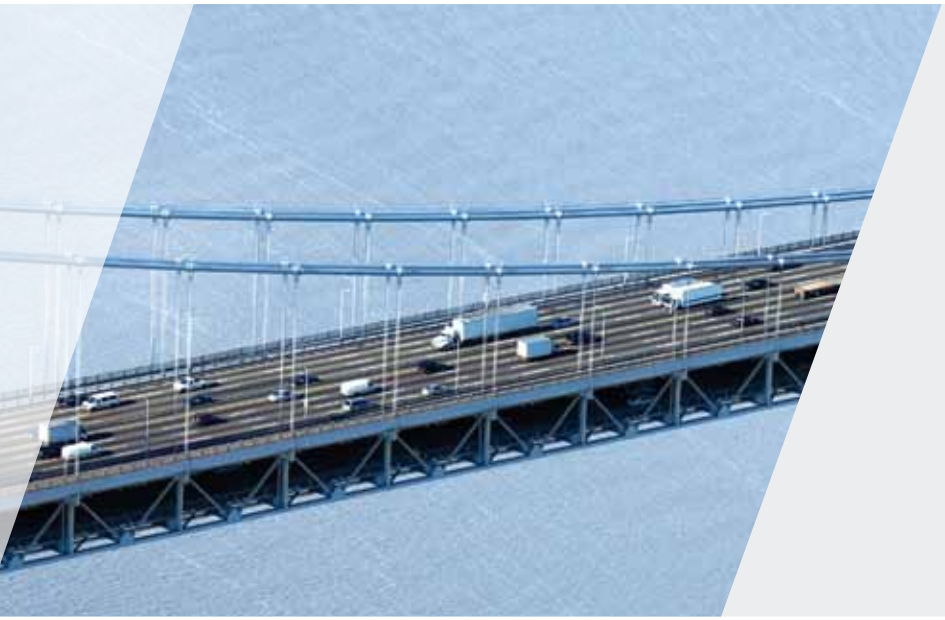
Threats and Vulnerabilities Are Accelerating





One in four survey respondents have been victims of extortion through cyberattacks or threatened cyberattacks.

One of the more startling results of our research is the discovery of the constant probing and assault faced by these crucial utility networks. Some electric companies report thousands of probes every month. Our survey data lend support to anecdotal reporting that militaries in several countries have done reconnaissance and planning for cyberattacks on other nations' power grids, mapping the underlying network infrastructure and locating vulnerabilities for future attack.



Cyberextortion

The threat of cyberextortion is widely acknowledged and has been rapidly increasing. Over a year, the number of companies subject to extortion increased by 25 percent. Extortion cases are equally distributed among the different sectors of critical infrastructure, signaling no one industry is immune to the reach of these cybercriminals. The countries of India and Mexico have a high rate of extortion attempts; 60 to 80 percent of executives surveyed in these countries reported extortion attempts.

Attacks Increasing

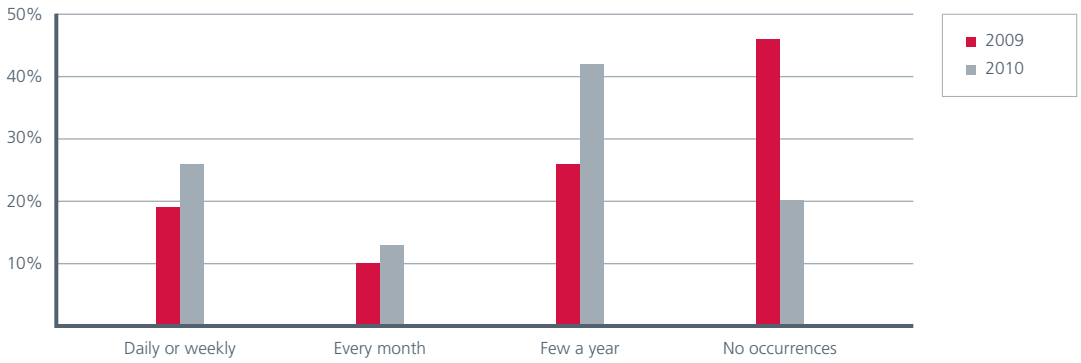
Just last year, nearly half of the respondents said that they had never faced large-scale denial of service attacks or network infiltrations. By this year, those numbers had changed dramatically; 80 percent had faced a large-scale denial-of-service attack, and 85 percent had experienced network infiltrations. Meanwhile, a quarter of our interviewees reported daily or weekly denial-of-service attacks on a large scale. A similar number reported that they had been the victim of extortion through network attacks or the threat of network attacks. Ominously, nearly two-thirds reported they frequently (at least monthly) found malware designed for sabotage on their system.

Extortion Widespread

Cyberextortion is already a big business. According to Allan Paller, Director of the SANS Institute, "Hundreds of millions of dollars have been extorted [from various companies], and maybe more […] This kind of extortion is the biggest untold story of the cybercrime industry."[2] Fully one in four of our respondents said they had already fallen victim to extortion through attack or threat of attack to IT networks in the last two years—up from one in five respondents a year ago.

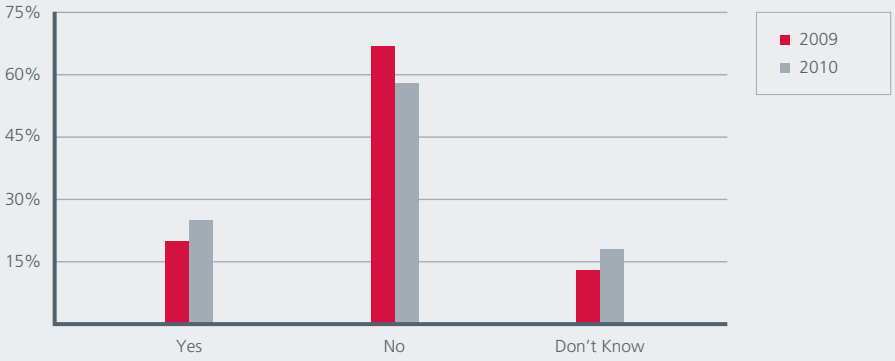
Extortion was pervasive in some countries, with 80 percent of respondents in Mexico and 60 percent in India reporting that they had been subject to

Threats & Vulnerabilities Accelerating



In 2010, 80% faced a large-scale denial of service attack, and 85% had experienced a network infiltration

Has your company been the victim of extortion through cyberattack or threat of cyberattack in the last two years?



cyberextortion attempts. This was a significant increase from 2009, when only 17 percent of Mexican respondents and 40 percent of those in India reported incidents of cyberextortion.

This evidence reinforced other reports suggesting that cyberextortion aimed at power systems is spreading. Cybersecurity officials outside Brazil have long suggested that the Brazil blackouts were caused by cyberexploits, despite Brazilian denials.[3] In any event, Brazil is not alone; statements by U.S. intelligence officials attribute power outages in several countries to cyberextortion.[4]

Stuxnet

For ordinary cybercriminals, shutting down a power system is more a sign of failure than of success. The whole point of cyberextortion is to get the victim to pay so that power will not have to be cut off.

Not so for cyberwarriors. The point of a state-sponsored attack would be to shut down or impair the infrastructure on which normal civilian life depends, diverting scarce resources, hurting civilian support for the war effort, and complicating military mobilization that depends on the civilian infrastructure. For years, industry spokesmen and techies who feared that acknowledging the risk would set the stage for new security regulation, discounted the risk of such an attack. Even those who saw the security holes in SCADA systems were inclined to shrug off the risk because there was no evidence that other nations would exploit those flaws for purposes of sabotage.

That debate ended, or should have, in the summer of 2010, when Stuxnet was identified. A remarkably sophisticated form of malware, Stuxnet had two characteristics that demonstrated the growing threat of cyberattacks.

First, Stuxnet had no obvious criminal payoff. It was designed for sabotage and sabotage alone. Stuxnet infects computer systems by exploiting a number of vulnerabilities on Microsoft Windows. Uploaded to the computer through, among other things, a USB drive, shared network files, or SQL databases, Stuxnet targets a specific Siemens SCADA program. If this software is running, Stuxnet looks for a particular configuration of industrial equipment and then launches an attack designed to manipulate certain microcontrollers to perform erratically while reporting normal functioning to operators of the system.

This is sabotage pure and simple. There is no easy way to use the malware either for espionage or for extortion. It has been widely speculated that Stuxnet was aimed at infiltrating Iran's heavily protected Natanz facility for enriching uranium. The delicate centrifuges at Natanz are crucial for Iran's nuclear weapons program, and they have suffered numerous unexplained failures since Stuxnet was launched.[5]

Stuxnet

Our data indicates that the Stuxnet virus did indeed have a global reach. Around 40 percent of respondents found Stuxnet on their computer systems. Stuxnet was more likely to appear in the electricity sector, where 46 percent of respondents found the malware.

Three-quarters of respondents who found Stuxnet were confident that the malware had been removed from their systems. However, action to neutralize Stuxnet varied widely from one country to another, and some of the countries with the higher rates of infection, like India, France, and Spain, also reported relatively low rates of countermeasure implementation.

57 percent of survey respondents launched special security audits because of concerns about Stuxnet.

Second, Stuxnet was an extraordinary advance in sophistication over the kinds of malware used by the criminal underground. The Belarusian security firm that initially identified Stuxnet at first believed it to be a backdoor for hackers. But closer inspection revealed the complex nature of the virus. It features multiple exploits that were previously unknown, has Microsoft Windows driver modules that had been signed using genuine cryptographic certificates stolen from respectable companies, contains about 4,000 functions, and uses advanced anti-analysis techniques to render reverse engineering difficult. It is almost certainly the work of a government, not a criminal gang.

Stuxnet is, in short, a weapon. It is a concrete demonstration that governments will develop malware to sabotage their adversaries' IT systems and critical infrastructure. It also shows that hostile governments can easily target the SCADA systems on which a nation's power, gas, oil, water and sewage systems depend, defeating the defenses upon which most companies rely.

According to one expert, most critical infrastructure systems were not designed with cybersecurity in mind. Within the electric sector, for example, the primary concern has always been maintaining a steady supply of power and an efficient system. Even today, many electric companies still use vendor-default passwords because they allow easy access in times of crisis or for maintenance and repair.

Recent power grid modernization efforts are in the same tradition. They have increased efficiency, and they have created new security holes. The consequences were demonstrated during tests conducted at Idaho National Labs in 2007. Researchers demonstrated that they could gain remote access to the control systems of a generator and remotely change its operating cycle, sending it out of control. A video of the incident shows the target generator shaking, smoking, and grinding to a stop. These generators are expensive, and they can take weeks or months to repair or replace.

The 2003 Northeast power blackout, although in no way connected to a cyberattack, showed how failure in even a small part of the grid can have cascading effects. The blackout affected 50 million people; although most saw power restored within 48 hours, some were left without electricity for up to a week.[6] The rate of failure was too fast for manual intervention: it took only seven minutes for the blackout to sweep across the region.[7]

The incident also shows the potential effectiveness of Stuxnet's "misreporting" feature, in which, reports one expert, activity is hidden from the network operations center, in an attack on energy and similar sectors. According to a report by the U.S.-Canada Power System Outage Task Force, which investigated the 2003 Northeastern U.S. blackout, owners of individual lines tried to tell control operators about the cascading failure but were ignored for some time because the control computers that monitored SCADA did not indicate any problems with power delivery. Only when other companies began calling attention to the problem did the workers realize the scope of the problem.[8]

"Nation states remain the number one threat to critical infrastructure cybersecurity in the United States," reports one industry expert. The only

Terrorist Attacks on the Grid?

If nation-states are a threat to civilian power and similar services, what about terrorists? Can they attack the grid and cause mass electrical outrages? With the possible exception of terrorists groups assisted by nation states, this threat is largely discounted by experts. "Attacking critical infrastructure is more bank-for-your-buck than attacking a military facility, but it still does not have the same emotional impact as images of carnage from a bombing of civilian targets," said one expert, though he cautioned that, as the current leadership of terrorist organizations is replaced by a younger generation, it is very likely that instances of cyberattacks will increase.

good news about that assessment is that government attacks may be less common than criminal extortion; "nation states are unlikely to [take] a practice shot," the expert believes.

In a conflict, though, cyberattacks seem probable. All major world powers have acquired or are in the process of acquiring cyberattack capabilities, and critical infrastructure remains a key target.

We asked industries dependent on SCADA systems whether Stuxnet had affected their operations. The answers are striking. Two-fifths of all respondents, and nearly half of those in the electric industry, said that they had found Stuxnet on their systems. In fact, the electric sector had the highest occurrence of Stuxnet among the critical infrastructure sectors surveyed. More than half of all respondents reported having to take action against Stuxnet.

Given the global distribution of our survey, these answers are remarkable. While quite possibly targeted at a single facility, Stuxnet chose a roundabout route to reach its target, essentially infecting everyone and then lying dormant if the system it infected did not have the particular configuration it was looking for. Perhaps for this reason, nearly three-quarters of respondents who encountered Stuxnet were confident or very confident that the malware had been removed or neutralized on their systems.

What conclusions did industry draw from the Stuxnet incident?

There is no doubt that the awareness of foreign government threats is high. Over half of the executives believe that foreign governments have been involved in network probes against their domestic critical infrastructure.

But the discovery of Stuxnet on their systems did not seem to galvanize companies to action. The highest levels of counter-Stuxnet security measures were implemented in the UAE, Italy, and Japan, where rates of Stuxnet infiltration were comparatively low. In contrast, countries such as India, where Stuxnet infiltration rates were high, exhibited comparatively low implementation of counter-Stuxnet measures.[9] As one expert from India explained, Stuxnet and other recent cyberincidents have raised awareness about cybersecurity, but without clear government policy on the issue, individual ministries and companies are left to implement their own measures. "There is nothing that adds up to a national picture, [and networks] continue to grow more and more vulnerable," the Indian expert said.

Many observers think that denial remains part of the industry's response to Stuxnet. According to one expert, many companies remain focused on resiliency in the event of a denial-of-service cyberattack, rather than a high-end attack intended to sabotage equipment, even though such an attack is fast becoming the leading threat to power and similar sectors. Said another source, "Stuxnet was a game-changer, but it will not change the direction in which U.S. cybersecurity legislation is moving" as policymakers have already recognized this threat; the larger problem lies in getting industry to recognize the changing nature of this threat.

"A lot of people still see [denial-of-service] as the main problem and they can deal with a DDoS incident, unless there is damage to the physical system. Getting them to perceive Stuxnet as a possibility is a huge issue," says an expert source consulted for this report. "The issue is not about the computer going away or not working, but rather about someone else using your computer to give different commands." The source cites the example of a hacking incident in the United States in recent years during which an individual was able to seize control of traffic lights and operate them at will.

Validating the source's concern, industry executives told us that they remained more concerned about DDoS attacks than about malware like Stuxnet. A third of respondents declared that they were not at all confident or not very confident in their company's ability to deal with DDoS attacks or stealthy infiltration. Asked about malware designed for sabotage, respondents expressed a similar lack of confidence only about 20 percent of the time. Yet, DDoS attacks are child's play to defend against compared to Stuxnet. "After Stuxnet, many people said, "I don't have Siemens, I'm not nuclear—I could care less," confirmed a U.S.-based cybersecurity expert.

Growing Vulnerabilities and Expectation of Attack

More than 40 percent of the executives we interviewed expect a major cyberattack within 12 months—an attack, that is, that causes severe loss of services for at least 24 hours, a loss of life or personal injury, or the failure of a company. This expectation is astonishingly high in some countries, notably India, where nine out of 10 executives said they expected such an attack within a year, and Mexico, where seven in 10 had the same expectation. Fear of a major attack was also relatively high in China, where over half of respondents expected such an attack in 2010 or 2011.

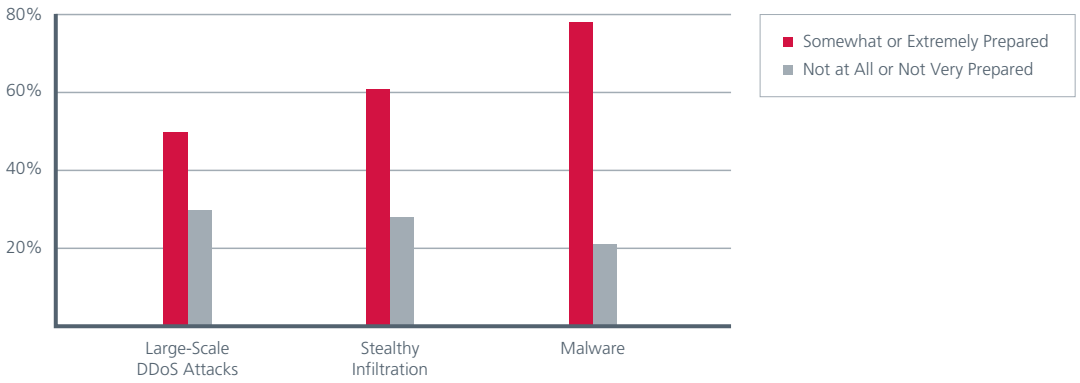
In some countries, perceptions of vulnerability were even more alarming. For example, three-quarters of respondents in Brazil, and 60 percent in Mexico, felt unprepared for a large-scale DDoS attack against their companies. Two-thirds of the companies in Brazil and Mexico also saw their systems as vulnerable to stealthy infiltration. The high levels of concern in Brazil may be attributable to the country's previous experience with cyberattacks and the sheer number of criminal hackers in Brazil (according to one study, one-third of the 50 most popular defacement websites are hosted and operated from Brazil[10]). In light of the 2005 and 2007 blackouts in major Brazilian cities, it is not surprising that 91 percent of Brazilian respondents believed their sector was unprepared for a malware attack.

Australian respondents were also surprisingly worried about their sector's vulnerability. Nine out of 10 respondents from Australia believed their sector was not at all or not very prepared for stealthy network infiltration. "There has been a very large government focus on Critical Infrastructure Protection in Australia. The growing sense of unpreparedness is the result of more understanding [of the threat] because of a big education effort for executives by the government," said Ajoy Ghosh, the chief information security officer for Logica Australia.

Growing Interconnectivity and the Smart Grid

Despite widespread industry unease about the growing vulnerability of the power grid, and the lack of preparedness for a network attack, power companies and governments seem to be doubling down on the danger.

How prepared are companies?



The most prominent initiative for electric utility networks today is not a major new drive to improve security; it is creation of a "smart grid." Smart grids use a two-way stream of information that allows the electricity supplier to monitor and control the flow of electricity to and sometimes inside the consumer's premises. The purpose of smart grids is to smooth demand by changing prices or even cutting off service to particular consumers or appliances when demand peaks, such as on late summer afternoons. Cutting peak demand means fewer power plants. Plans to exercise far more precise control over consumers' use of electricity has aroused great enthusiasm among government policymakers, particularly in China and the United States.

Global smart grid spending will exceed $45 billion by 2015.[11] At the same time, customers and consumer groups have raised concerns about what the smart grid will mean for energy prices and privacy.[12] Lew Owens, CEO of South Australia's privately owned electricity distributor ETSA, acknowledged as much to the Australian Broadcasting Corporation: "The words 'smart meter' sound fantastic […] But what it actually is saying is that we will force people to reduce their consumption by making the price so great that they […] turn it off."[13]

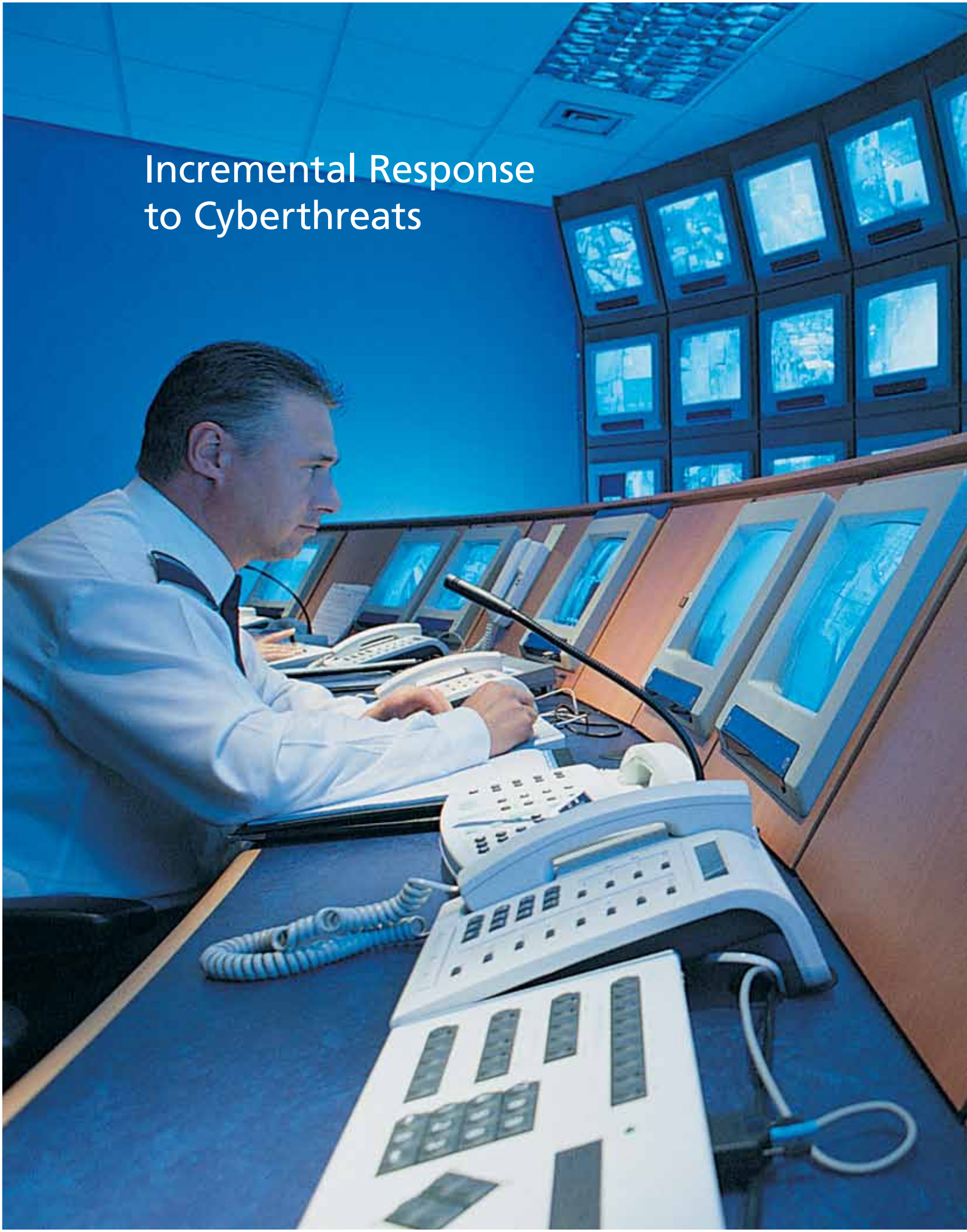
Our data nonetheless show an industry that is charging ahead with smart grid implementation. Four out of five industry executives said their company intended to implement some form of smart grid controls, such as time-sensitive rates, service cutoffs, and service reductions.

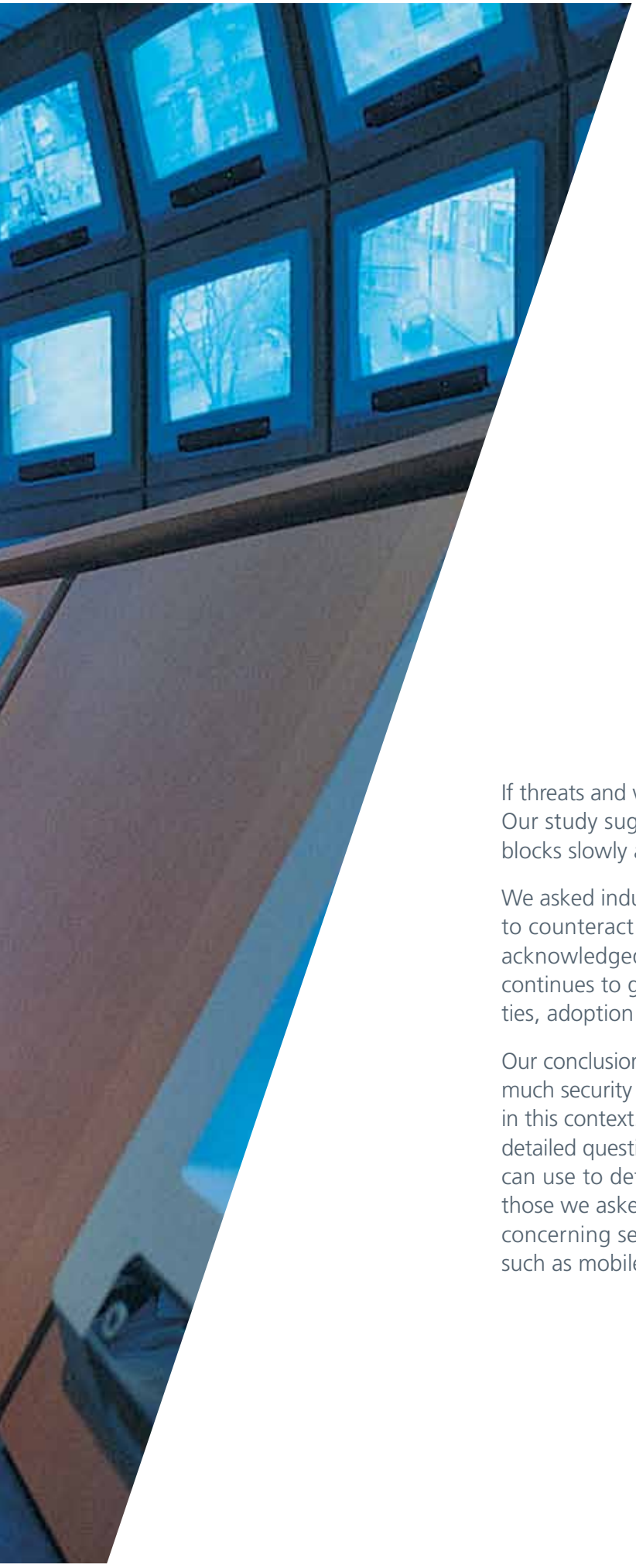
But extending network control to the household or even the appliance level will create new opportunities for harm if the network itself is not secure. If the new smart meters or the network that supports them can be taken over by attackers, they will be used to disrupt the delivery of electricity in a fine-grained way, singling out particular users or even appliances for power cuts or perhaps surges. As explained by a security expert, "Systems are increasingly vulnerable due to automation and remote accesses, as there are more access points from which to launch attacks. Also, the ways we change are impaired and slow, so we remain vulnerable for longer."

Most executives and outside observers do not believe that the networks controlling power systems are secure today, particularly against state-sponsored attacks. At least one executive we interviewed decried "the dumbness of 'let's put every household's power supply on the Internet—and call it smart'!"

Certainly there is room to question just how secure the new systems will be. More than half (56 percent) of the executives whose companies are planning new smart grid systems also plan to connect to the consumer over the Internet. Most realized that the new systems will add challenging security vulnerabilities to an already threatened electric network, but only two-thirds have adopted special security measures for the smart grid controls. According to Jim Woolsey, former United States Director of Central Intelligence, "Ninety to 95 percent of the people working on the smart grid are not concerned about security and only see it as a last box they have to check.

Incremental Response to Cyberthreats





The good news is that adoption of security measures continues to grow. The bad news is that, unlike threats and vulnerabilities, adoption of new security measures is improving at a snail's pace.

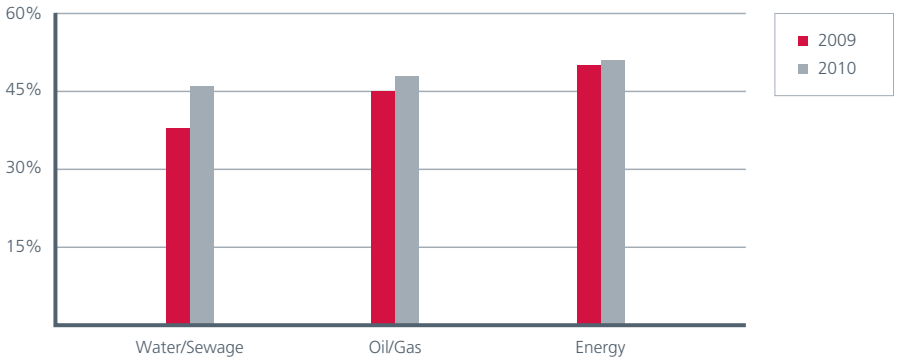
If threats and vulnerabilities are growing, what about security measures? Our study suggests that investment in security is coming out of the blocks slowly at best.

We asked industry executives what security measures they were taking to counteract the vulnerabilities and threats that so many of them acknowledged. The good news is that adoption of security measures continues to grow. The bad news is that, unlike threats and vulnerabilities, adoption of new security measures is improving at a snail's pace.

Our conclusion is not based on executives' subjective assessment of how much security they are providing. Subjective judgments are not reliable in this context. To find a more objective standard, we asked IT executives detailed questions about 29 different security measures that companies can use to defend their networks. These questions were similar to those we asked in the past report, but this year also included questions concerning security challenges posed by new technology initiatives, such as mobile phone access and IP connections.

These security measures included security technologies, security policy, encryption, authentication, and network connectivity. Because this year's list of possible security measures greatly overlapped last year's, we were able to assemble a rough guide to how much progress companies had made in increasing security. This "security measure adoption rate" is only a rough guide, since network security does not depend on simply piling one security technology on top of another and because not all security technologies are equally effective. Nonetheless, this rate does provide some sense of whether the industry is in fact adding new security measures in response to new threats and vulnerabilities.[14]

Measuring improvement: Security measure adoption rates



And that is indeed what industry is doing, though slowly. In each of the sectors we examined, the executives reported adopting a larger number of security technologies this year than last. The water and sewage sector, which had much lower than average rates of security measure adoption in 2009, improved markedly from 38 percent to 46 percent. Oil and gas executives reported adoption of 48 percent of available technologies, up from 45 percent the year before. And energy companies, which led the field in security adoption last year, largely rested on their laurels this year, increasing security measure deployment only a point, from 50 percent to 51 percent.

Despite the increases, the fact remains that most companies failed to adopt many of the available security measures. This means that, for many, security remained rudimentary. For instance, 44 percent of those surveyed reported only using username and password ("shared secret") authentication for on-site network access. By contrast, less than one in five respondents used only tokens, while 3 percent only relied on biometric measures. Less than one in ten reported using all three methods for on-site network access purposes.

Security Measures Counted:

- Software maintenance and security patches
- Standardized desktop configuration
- Sharing information with industry/ government partners
- Threat-monitoring service subscription
- Bans or restrictions on USB devices or other removable media
- IT network authentication with shared secrets, tokens, or biometric identifies
- Offsite IT network authentication with shared secrets, tokens, or biometric identifiers
- Firewalls to public networks
- Network access control measures
- Database-specific security and access controls
- Intrusion prevention systems
- Intrusion detection systems
- Firewalls between corporate systems
- Security information management tools
- Data loss prevention tools
- Role and activity anomaly detection
- Application whitelisting
- Tools to monitor network activity
- Encryption use (in online transmission, data stored in the network, laptop hard drives, databases, emails, and portable mechanisms)
- Regulation of mobile devices (anti-virus software, reflash, not attached to the network)
- Monitoring of new IT network connections through audits or network behavior analysis tools

Security measure adoption rates reported by country

Offsite access was only slightly more restricted: 26 percent of respondents used only passwords, while about one-fifth only relied on tokens and a tiny 3 percent only used biometric authentication. Only about one in 10 respondents reported that off-site network access was entirely prohibited.

More sophisticated security measures, such as tools to monitor network activity or to detect role anomalies, were adopted by a distinct minority (25 percent and 36 percent, respectively) of the respondents. Yet, these measures prove most effective and most necessary for network security, confirmed one cybersecurity expert. "The focus is now on audits, things that keep track of what is normal, and developing components that are smarter and more resilient," he stated. Measured objectively, some countries are clearly more security conscious than others. Last year, China was a standout, well ahead of all other countries in adoption of security measures. This year the figures tell much the same story. China maintained its position as the country with the highest security adoption rate overall at 59 percent, followed by Italy and Japan at 55 percent and 54 percent respectively. In contrast, Brazil, France, and Mexico had the lowest security adoption rates, close to half the rate shown by the leaders. The remaining countries were grouped closely together around the median score of 43 percent.

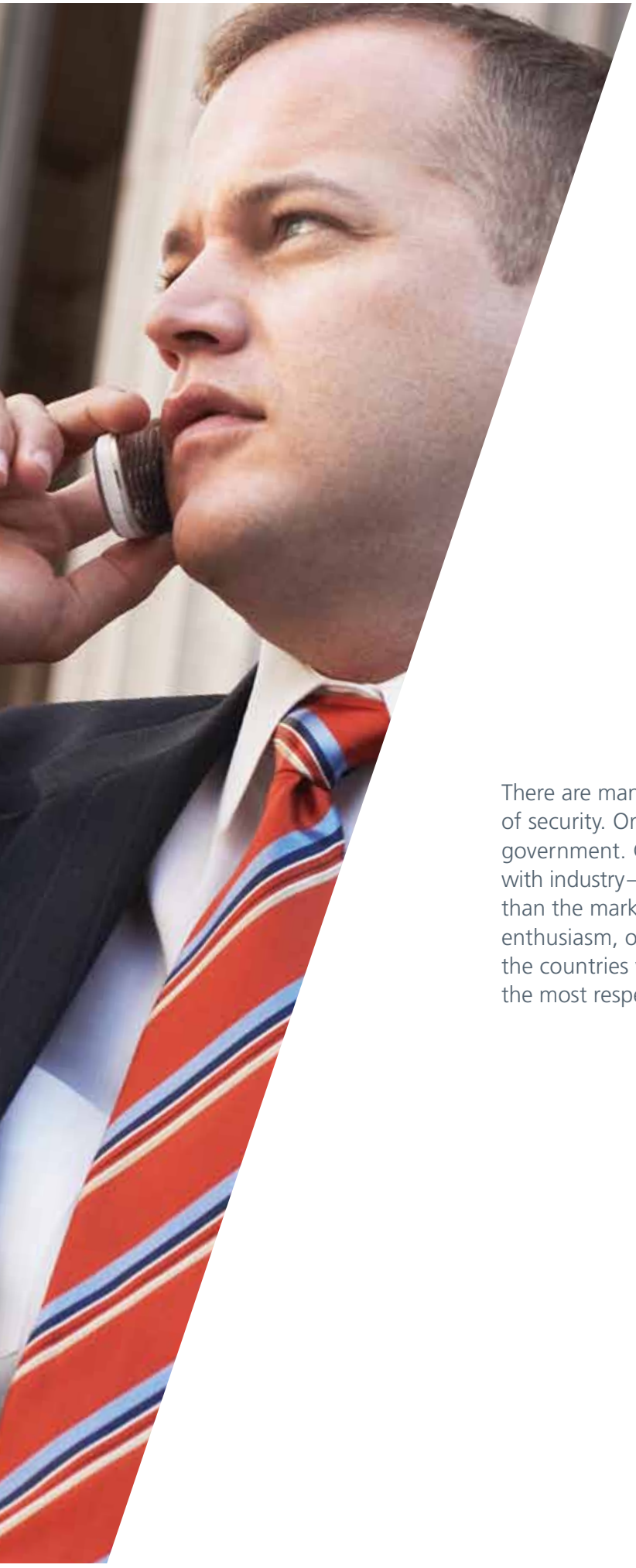
32 percent of companies surveyed have not adopted special security measures for smart grid controls.

Opposite Ends of the BRIC

Despite their shared position as emerging global leaders, the cybersecurity policies of Brazil and China could not be more different. At one end, Brazil demonstrated a series of contradictions between threat perceptions and responses. The country consistently ranked last in terms of security measure adoption and reported one of the highest perceived vulnerability rates of all countries polled. The Brazilian authorities also carried one of the lowest trust levels from those surveyed. Yet Brazil—a country with documented instances of cyberextortion attack—also had one of the lowest attack anticipation rates; only about one-third of respondents feared a major cyberincident in the next 12 months.

On the other hand, China remained a leader in security measure adoption and maintained a strong level of confidence associated with the Chinese leadership's ability to prevent and deter cyberattacks. The government has taken an active role in responding to the cybersecurity crisis, allowing China to surpass other developing countries in terms of network security, and narrow its gap with security leaders in the developed world. This suggests that despite shortcomings, China appears to have a plan regarding cybersecurity. Nonetheless, the country continues to face an enormous cybersecurity challenge on account of the prevalence of pirated software. As stated by one expert, "If 90 percent of all software in a given country has been pirated, it really does not matter what security measures the government implements—a critical vulnerability remains."

Government Response



Government can encourage security by collaborating with industry—and by adopting regulations that demand better security than the market does.

There are many reasons for the divergence among countries in terms of security. One is almost certainly the difference in the role played by government. Government can encourage security by collaborating with industry—and by adopting regulations that demand better security than the market does. Some governments have played these roles with enthusiasm, others with diffidence. In the end, perhaps surprisingly, the countries with the most active regulatory regimes tended to earn the most respect and confidence from private industry.

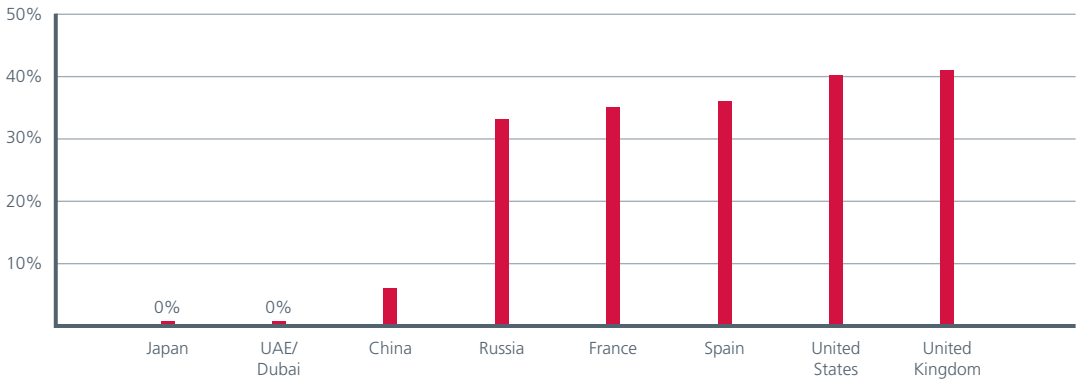
Role of Government

To measure public-private relationships, we asked IT executives how they interacted with government, suggesting many alternatives, including no interaction at all, informal information-sharing, and regulatory oversight.

Chinese executives were at the top of the scale—reporting high levels of both formal and informal interaction with their government on security topics.[15] By the same token, only a handful of Chinese executives (about one in 20) said that they had no contact with government agencies regarding network security—one of the lowest non-involvement rates in any country.

The other country with high public-private interaction was Japan, where cybersecurity oversight seems to have increased significantly over the last year. Nearly half (44 percent) of Japanese respondents reported that government agencies exercised extensive or detailed regulatory authority over their network defense measures, a regulatory reach that exceeded even that of China, where 28 percent of respondents said that they were regulated in detail. Equally striking, about nine out of 10 Japanese respondents reported cooperating and consulting with government through public-private partnerships, far more than any other nation. One Japanese security expert attributed this high level of cooperation to the unique nature of Japan's

Percentage reporting they do not interact with their government on cybersecurity or defense matters



Government audits

public-private cybersecurity partnership: "The feature of our public-private partnership is that government encourages the autonomy of critical infrastructure owners and operators [and] supports their self-motivating activities rather than regulating them."

On the other end of the spectrum were countries like Spain, the United States, and the United Kingdom, where more than a third of all respondents reported no contact with government on cybersecurity, with most of the remainder saying they had only informal exchanges on the topic.

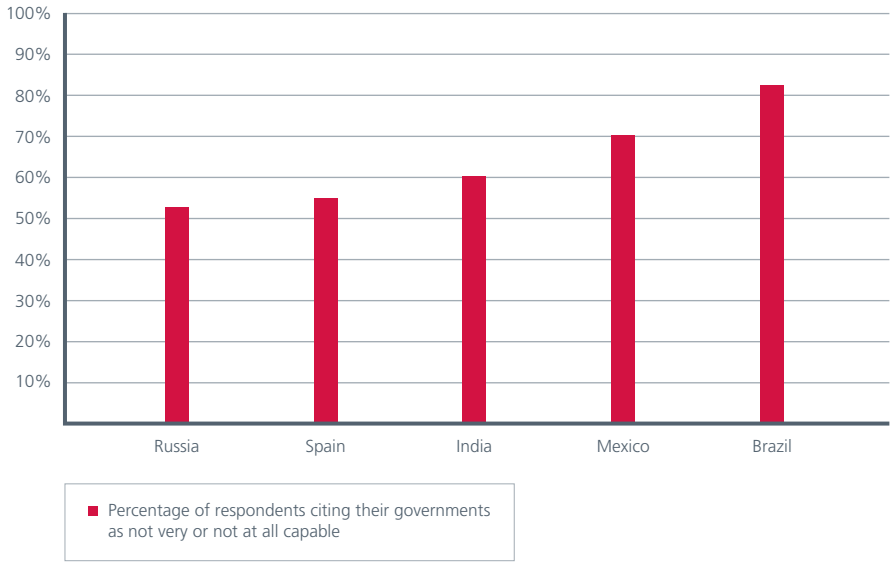
An almost identical pattern emerged when we asked IT executives whether their security plans were audited by government Every one of the Japanese respondents reported undergoing such audits. This is a significant increase for Japan over last year, when China led in security audits. This year, China ranked second in auditing, with seven of 10 respondents reporting such audits. The lowest audit rates occurred in the United Kingdom, Spain, and the United States, which all scored below 20 percent.

Between last year and this year, some countries seem to have greatly expanded the reach of their security audits while other countries seem to have cut back. In 2009, the gap between the country experiencing the most government audits and the country with the least was 50 percentage points. That is a hefty margin. But in 2010, the margin had ballooned to ninety-four points, the difference between Japan's 100 percent audit and the UK's six percent.

Based on these figures, if there is a race among governments to harden their civilian infrastructure against cyberattack, Europe and the United States are falling behind Asia.

Twenty-five percent of critical infrastructure companies do not interact with the government on cybersecurity and network defense matters.

Perceptions of government *incapability* to prevent or deter cyberattack



Overall Confidence in Authorities

We also asked IT executives how much confidence they had in the ability of the authorities to prevent and deter potential cyberattacks. Their answers remained virtually unchanged from 2009. This year, 54 percent of respondents reported that authorities are "mostly capable, capable, or completely capable" of preventing or deterring attacks, similar to the 55 percent who offered the same assessment in 2009.

Evaluations of particular countries' capabilities varied substantially, as in the past. Japan's increased focus on regulation and audits may have spurred a new view of the government's capabilities, with 83 percent stating confidence in the authorities this year, compared to 56 percent in 2009.

"No confidence" votes were highest for Brazil, Mexico, and India, where confidence in government fell from 2009. This lack of confidence may be at least partially attributed to a limited auditing regime. According to one expert, the sporadic nature of security audits in India often leads to a false sense of security. "This is such a dynamic sector that audits performed six or eight months ago are no longer valid. What is needed is a continuous three-month auditing timeline [cycle] and a system of surprise checks," said one Indian expert.

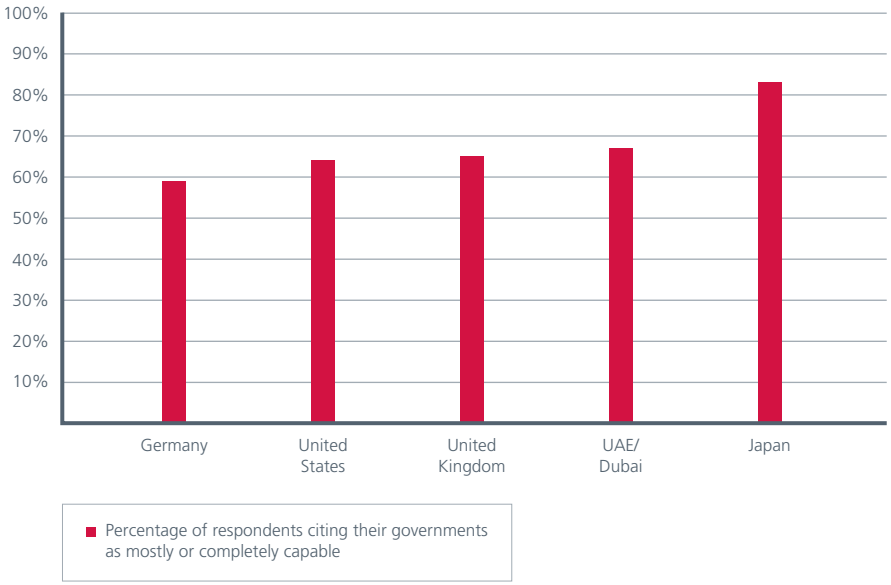
A broadly similar pattern held true when we asked whether respondents believed that current law was sufficient to prevent or deter attacks. The highest levels of confidence were found in Japan (78 percent), the UAE (67 percent), and China (56 percent). Brazil had the lowest levels of confidence, with less than one in five respondents reporting trust in authorities. Italy, Mexico, and Australia also voiced low confidence in the ability of laws and regulations to address cyberincidents. The surprise was India, which expressed great confidence (90 percent) in the ability of laws to deter cyberattack, despite the Indian respondents' otherwise low expectations for government institutions.

Government as Attacker

Governments also play another, more notorious role in cybersecurity. Their intelligence and military arms infiltrate and prepare to attack the networks of other countries. During the interviews conducted for this report, the cyberthreat that was cited most often was government-sponsored sabotage and espionage.

During the interviews conducted for this report, the cyberthreat that was cited most often was government-sponsored sabotage and espionage.

Perceptions of government *capability* to prevent or deter cyberattack



"The focus today is on resiliency, but what about espionage?" said a senior U.S. Senate staffer. "This is a major issue that needs to be addressed; denial-of-service is not the most significant problem." Many cybersecurity experts share concerns about surveillance of the U.S. power grid by other nation states. A classified 2008 Defense Science Board Report also highlighted the vulnerability of the U.S. electrical grid to cyberattack, and senior military officials have said publicly that potential opponents had engaged in cyber-reconnaissance of American critical infrastructure electrical utilities to plan for attack.

For two years in a row, we have asked IT executives in critical infrastructure sectors whether they believe that they have been subject to government infiltration or attack and if so, which countries are of greatest concern in that context. For two years in a row, the number of perceived nation-state attacks has remained stable and high, with almost three-fifths of the executives saying that foreign governments had been involved in network attacks against their domestic critical infrastructure.

What has changed, however, is the countries drawing the greatest attention and concern. In 2009, the United States was the country most often cited, just ahead of China. Both were concerns for about a third of the executives who believed their sectors were being attacked.

This year, though, China stands alone. Roughly the same percentage of respondents (30 percent) still cite China as a major source of concern for cyber-attack. What has changed is that concern about the United States has declined dramatically—from 36 percent to 12 percent. Meanwhile, Russia, (16 percent), North Korea (11 percent) and India (4 percent) placed relatively high, as IT executives in the sector have begun to appreciate how widely cyberattack technology has proliferated.

The variations in perceived threat origins followed a regional concentration pattern across all geographic areas surveyed. Not surprisingly, respondents in the Asia-Pacific region viewed China, Russia, North Korea and the United States as the largest threat sources. Within this group, fully two-thirds of Japanese respondents identified either China or North Korea as the main source of cyberthreat.

What country is of greatest concern in the context of network attacks on your country or sector?

The variations in perceived threat origins followed a regional concentration pattern across all geographic areas surveyed.

In the case of Australia, 40 percent of respondents viewed Russia as the main concern. The only country to break from this regionally-based perception was unsurprisingly China, where three-quarters of those polled most feared the United States.

Results from other regions also pointed to geographically-based threat perceptions. Two-thirds of those polled in the UAE most feared other Middle Eastern countries. European respondents were most concerned about China, Russia, North Korea, and the United States while Russia also weighed most heavily on the minds of Indian respondents. Interestingly, only 14 percent of Indian survey-takers were concerned about China, while almost a third feared the United Kingdom.

In the western hemisphere, the United States was most concerned about China. Although respondents in Latin America put forth one of the most diverse lists of threat origins, three-quarters of those surveyed in Brazil and over half of those polled in Mexico identified China or Russia as the main sources of cyberthreat. This perception corresponded to one of the highest rates of reported network penetration; overall, Mexico and Brazil emerged as two of the most vulnerable survey respondents, with serious concerns regarding their countries' response capabilities against all forms of cyberincidents, especially stealthy infiltration and DDoS attacks.

Recommendations

The emergence of Stuxnet points to an overriding need for critical infrastructure companies to acknowledge the changes in the cyberthreat landscape and focus attention not only on denial-of-service attacks, but also on more sophisticated threats, like stealthy infiltration from state-sponsored actors or cyberextortionists. As our research has shown, the critical infrastructure sector has been slow to adjust to this realization. To meet the challenges of the changing environment, true critical infrastructure protection policies must include updated threat responses focused on the following:

- Improved authentication measures, moving away from passwords to a higher reliance on tokens and biometric identifiers
- Better hygiene of network systems to include increased use of encryption technologies and the monitoring of network use activities for role and activity anomaly detection
- Increased oversight of access to industrial control systems, including how they access the Internet, through the oversight and active management of Internet connections, mobile devices, and removable media
- Effective partnerships with governments. The nature of these partnerships will vary from country to country and range from encouragement to mandatory action, but the nature of the new threats industry faces requires government involvement.

Conclusion

Overall, we found little good news about cybersecurity in the electric grid and other crucial services that depend on information technology and industrial control systems. Security improvements are modest and overmatched by the threat. Much as they may suffer from distributed denial of service attacks, these industries suffer even more from what might be called a "distributed denial of attack." Very few companies are rising to the challenge posed by state-sponsored infiltration and potential attack. That is particularly true in the Western Hemisphere, India, and Europe. In East Asia, government regulators seem to be pursuing a more concerted campaign to bolster security substantially.

Denial is an unrealistic long-term strategy. Whether audits and similar regulation will work better remains to be seen, but we can no longer pretend that it is business as usual for cybersecurity.

Other observers believe that even more action is needed. "Regulated enforcement of existing capabilities is not likely [to solve the problem]," says Jim Woolsey. "The real answer is new technology and distributed generation. Whatever encourages innovation and distributed generation is a step in the right direction." Whether Woolsey is right and new technologies can solve this problem or whether improved regulation offers the best chance for greater security, this study shows that steps to better security lie well in the future—and may have to wait until an unprepared population has suffered from cyberattacks on power, oil and gas, or water and sewer systems.

Acknowledgements

The survey was carried out in November 2010 by Vanson Bourne. The respondents were drawn from 14 countries, including Australia, Brazil, China, France, Germany, India, Italy, Japan, Mexico, Russia, Spain, the United Arab Emirates/Dubai, the United Kingdom, and the United States.

The authors of this report would like to thank all those who contributed and shared their expertise and insights with the writers of this report.

Endnotes

1 These are the systems that control power grids, refineries, water, sewage, and other industrial processes.

2 Duclos, Susan. "Cyber Attacks Black Out Cities Outside the U.S.—Cyber Terrorism," *Digital Journal*, January 19, 2008. *http://www.digitaljournal.com/article/249107?tp=1.*

3 *Cyber War: Sabotaging the System.* Prod. Graham Messick. CBS: 60 Minutes, 2009. 8 Nov. 2009. Web. 3 Jan. 2011. *http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.* Harris, Shane. "Brazil to "60 Minutes": It Wasn't A Hacker." *The Atlantic.* 10 Nov. 2009. Web. 3 Jan. 2011. *http://www.theatlantic.com/politics/archive/2009/11/brazil-to-60-minutes-it-wasnt-a-hacker/29934/.*

4 SANS NewsBites, Volume X, Issue 5, January 18, 2008. *http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5&rss=Y*

5 William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, January 15, 2011. *http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html*

6 Kaplan, Stan Mark. *Electric Power Transmission: Background and Policy Issues.* Reports and Issue Briefs. Washington, D.C.: Congressional Research Service, 2009.

7 Michael Giberson, Lynne Kiesling. "Analyzing the Blackout Report's Recommendations: Alternatives for a Flexible, Dynamic Grid." *Electricity Journal* 17.6 (2004): 51–59.

8 U.S.-Canada Power System Outage Task Force, "Context and Preconditions for the Blackout: The Northeastern Power Grid Before the Blackout Began," *August 14th Blackout: Causes and Recommendations*, p. 53. *https://reports.energy.gov/B-F-Web-Part2.pdf*

9 Australia and Italy tied for fifth place with 40 percent of respondents reporting Stuxnet incidents. This can be compared to 100 percent of Indian respondents, 59 percent of German and French respondents, 45 percent in Spain, and 44 percent in China reporting Stuxnet infiltration.

10 Mylrea, Michael, "Brazil's Next Battlefield: Cyberspace," The Fletcher School, November 15, 2009. *http://fletcher.tufts.edu/news/2009/11/opeds/Mylrea-Nov15.shtml*

11 ABI Research: *http://www.abiresearch.com/research/1005219.* Cited here: *http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100708005824&newsLang=en*

12 Peeples, Doug. "Anti-Meter Fever Strikes Australia Too," *Smart Grid News.com*, February 24, 2010. *http://www.smartgridnews.com/artman/publish/Technologies_Metering_News/Anti-Meter-Fever-Strikes-Australia-Too-1926.html*

13 ABC Radio National, "Electric shocks," November 5, 2006. *http://www.abc.net.au/rn/backgroundbriefing/stories/2006/1777438.htm*

14 We asked separately about adoption of security measures for critical IT networks and for SCADA/ICS systems, but the resulting patterns were so similar in each case that we discuss here only the security measures for critical networks.

15 The categories included: "by participating in industry information sharing associations"; "by providing public comment on changes to regulation/legislation"; "by actively lobbying through industry groups regarding regulation/legislation"; and "by consulting through government-private sector partnership organizations."

About the authors

Stewart Baker is a distinguished visiting fellow at the Center for Strategic and International Studies and a partner in the Washington law firm of Steptoe & Johnson. From 2005 to 2009, he was assistant secretary for policy at the U.S. Department of Homeland Security. Prior to that, he served as general counsel to the Silverman-Robb Commission, investigating the failures of U.S. intelligence on Iraqi WMD. From 1992 to 1994, he was general counsel of the National Security Agency.

Natalia Filipiak is a program manager and research associate in the Technology and Public Policy Program at the Center for Strategic and International Studies. She holds a master's degree in international relations from the Johns Hopkins University School of Advanced International Studies.

Katrina Timlin is a research assistant in the Technology and Public Policy Program at the Center for Strategic and International Studies. She graduated Phi Beta Kappa from the George Washington University with a B.A. in International Affairs.

The Center for Strategic and International Studies (CSIS) provides strategic insights and policy solutions to decision makers in government, international institutions, the private sector, and civil society. A bipartisan, nonprofit organization headquartered in Washington, DC, CSIS conducts research and analysis and develops policy initiatives that look into the future and anticipate change.

For more information about CSIS, visit: www.csis.org.

McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

For more information, visit: www.mcafee.com.

McAfee
2821 Mission College Blvd.
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

21900rpt_cip_0311