



In the Crossfire

Critical Infrastructure in the Age of Cyber War

A global report on the threats facing key industries



In the Crossfire

Authors:

Stewart Baker, distinguished visiting fellow,
CSIS; partner, Steptoe & Johnson

Shaun Waterman, writer and researcher, CSIS

George Ivanov, researcher, CSIS

CONTENTS

Introduction	1
The Threat is Real	2
Responding to the Threat—Resources and Preparedness	12
Countering the Threat—Security Measures	18
The “State of Nature” and the Role of Government	24
Improving Security in an Age of Cyber War	32
Acknowledgements	40

Introduction and Background of the Study

In an ever more networked world, the cyber vulnerabilities of critical infrastructure pose challenges to governments and owners and operators in every sector and across the globe.

With the global economy still fragile after last year's financial crisis, assuring the integrity and availability of key national industries may fall out of focus as a government priority, but will remain a key determinant of strategic vulnerability.

Six hundred IT and security executives from critical infrastructure enterprises across seven sectors in 14 countries all over the world anonymously answered an extensive series of detailed questions about their practices, attitudes and policies on security—the impact of regulation, their relationship with government, specific security measures employed on their networks, and the kinds of attacks they face.

Critical infrastructure owners and operators report that their IT networks are under repeated cyberattack, often by high-level adversaries. The impact of such attacks is often severe, and their cost is high and borne widely.

Although executives generally report satisfaction with the resources they have for security, recession-driven cuts have been widespread and sometimes deep. And there is concern about how well-prepared critical infrastructure is to deal with large-scale attacks.

By gathering details on the actual security measures that organizations adopted, we were able to make an objective comparison of security in different critical infrastructure sectors, and in different nations. The executives with responsibility for operational or industrial control systems were also asked a series of special questions about the security measures employed on those systems.

Executives in China reported by far the highest rates of adoption of security measures including encryption and strong user authentication. Among sectors, water/sewage executives reported the lowest rate of adoption of security measures.

Broken down by sector and by nation, the survey data reveals significant variations in attitudes to and reports about regulation and other government activity. Executives in India reported the highest

levels of regulation, closely followed by China and Germany. Executives in the United States reported the lowest levels. Views about the impact and effectiveness of regulation varied widely, but overall most agreed that they improve security.

A majority of executives believed that foreign governments were already involved in network attacks against their country's critical infrastructure. The United States and China were seen as the most worrisome potential cyber aggressors, but attribution challenges in cyberspace give all attackers "plausible deniability."

Methodology

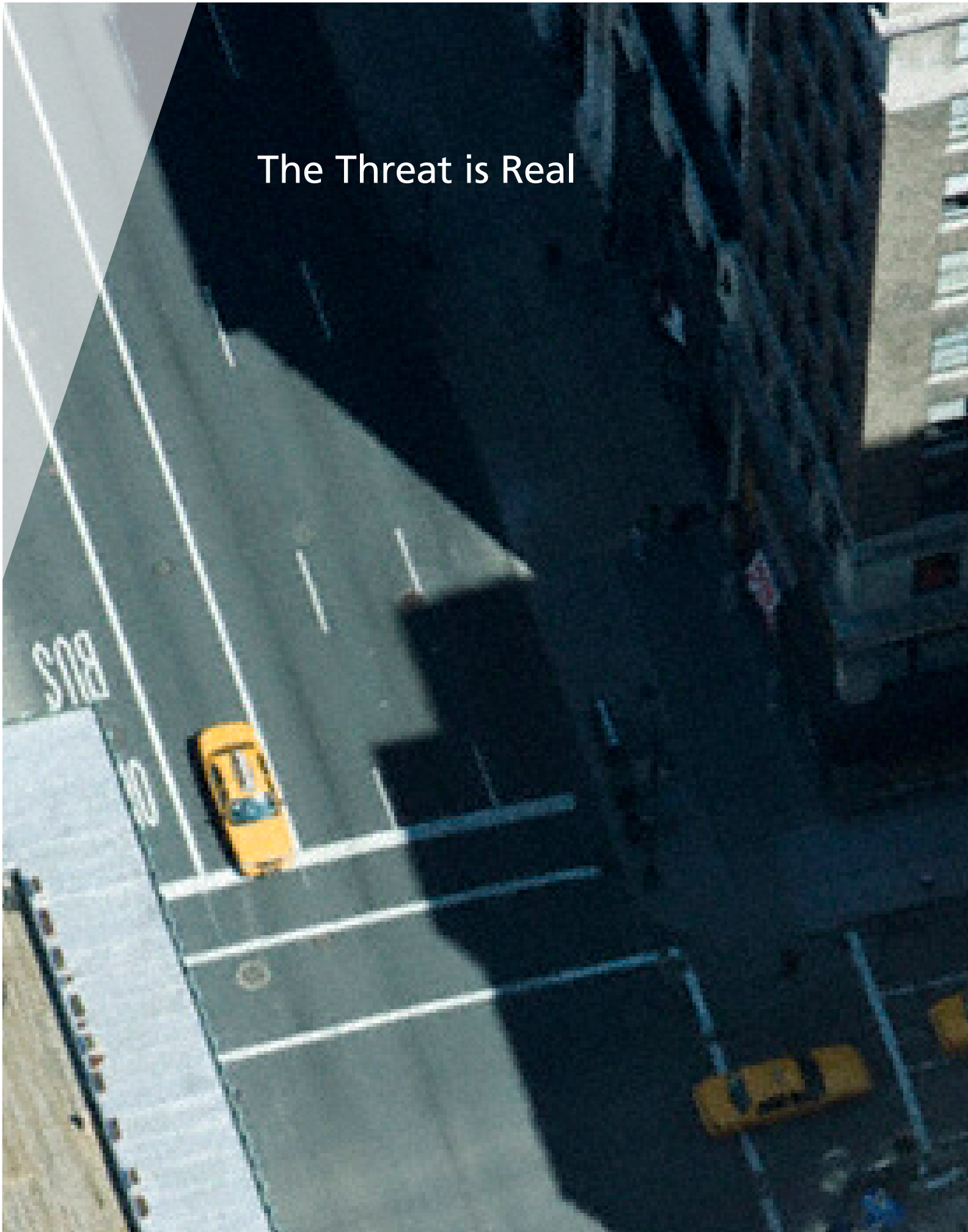
The survey data gathered for this report paints for the first time a detailed picture of the way those charged with the defense of critical IT networks are responding to cyberattacks, attempting to secure their systems and working with governments. A team from the Technology and Public Policy Program of the Center for Strategic and International Studies in Washington, DC analyzed the data, supplemented it with additional research and interviews, and wrote this report.

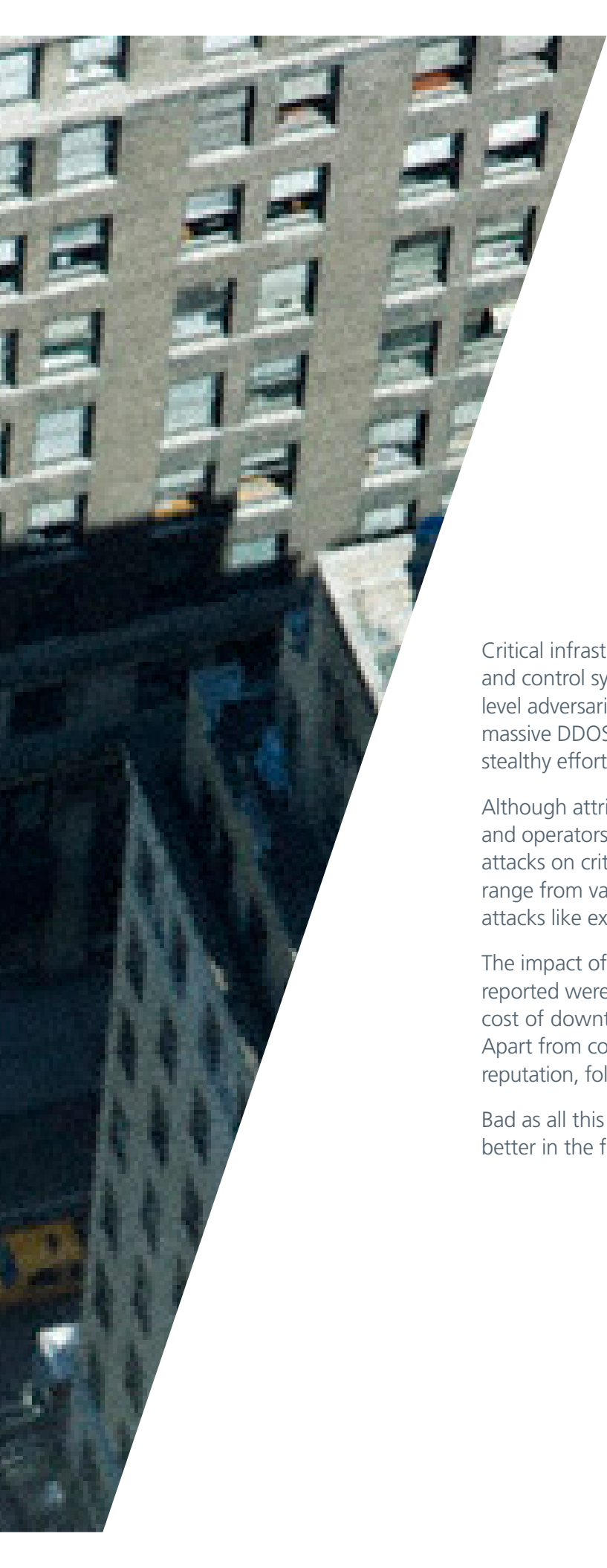
The respondents are executives who have IT, security or operational control systems responsibilities with their organization. About half said they had responsibility for such functions at a business unit level, with a quarter reporting their responsibilities were at the global level.

The survey was not designed to be a statistically valid opinion poll with sampling and error margins. It is rather a rough measure of executive opinion, a snapshot of the views of a significant group of decision-makers.¹

The CSIS team used interviews to provide context, background and verification for the survey data—adding detail to the picture of regulatory environments and threat/vulnerability levels across all seven sectors in each country, and discussing best practices. Many interviewees declined to be quoted by name, some declined to be named or quoted at all. All those who agreed to be identified are thanked in the acknowledgements.

The Threat is Real





Networks and control systems are under repeated cyberattack, often from high-level adversaries like foreign nation-states.

Critical infrastructure owners and operators report that their networks and control systems are under repeated cyberattack, often from high-level adversaries like foreign nation-states. Assaults run the gamut from massive DDOS attacks designed to shut down systems all the way to stealthy efforts to enter networks undetected.

Although attribution is always a challenge in cyberattacks, most owners and operators believe that foreign governments are already engaged in attacks on critical infrastructure in their country. Other cyberattackers range from vandals to organized crime enterprises. Financially motivated attacks like extortion and theft-of-service are widespread.

The impact of cyberattacks varies widely, but some of the consequences reported were severe, including critical operational failures. The reported cost of downtime from major attacks exceeds U.S. \$6 million per day. Apart from cost, the most widely feared loss from attacks is damage to reputation, followed by the loss of personal information about customers.

Bad as all this is, respondents believe the situation will get worse not better in the future.



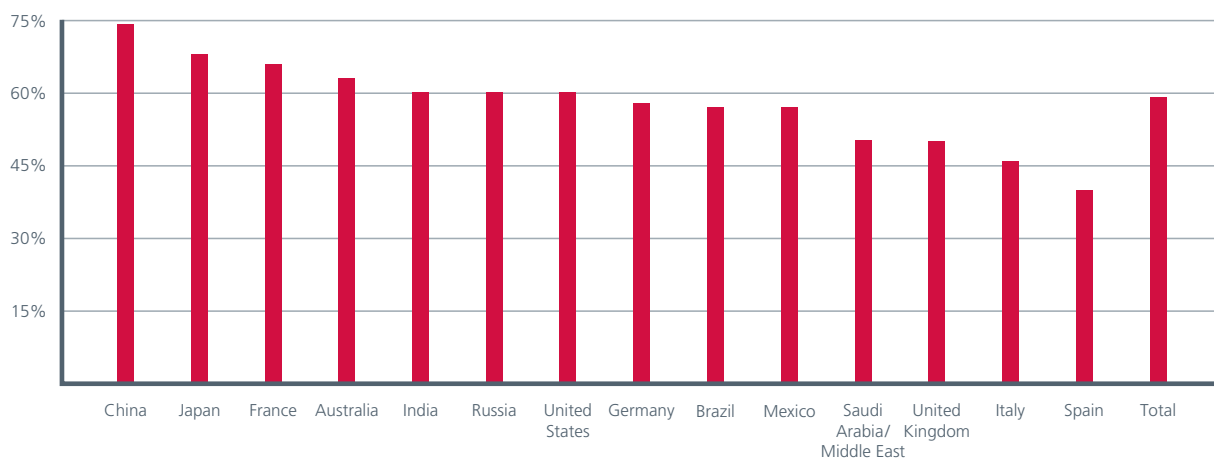
Serious cyberattacks are widespread

More than half of the executives surveyed (54 percent) said they had experienced “Large-scale denial of service attacks by high level adversary like organized crime, terrorists or nation-state (e.g. like in Estonia and Georgia).” The same proportion said they had been subject to “stealthy infiltration” of their network by such a high-level adversary “e.g. like GhostNet”—a large-scale

spy ring featuring individualized malware attacks that enabled hackers to infiltrate, control, and download large amounts of data from computer networks belonging to non-profits, government departments and international organizations in dozens of countries.

A hefty majority (59 percent) believed that representatives of foreign governments had already been involved in such attacks and infiltrations targeting critical infrastructure in their countries.

Percentage believing foreign governments have been involved in cyberattacks against critical infrastructure in their country





A majority believe foreign governments are already involved in cyberattacks on critical infrastructure.

In 2007, McAfee's annual Virtual Criminology Report concluded that 120 countries had, or were developing, cyber espionage or cybe war capabilities. Authorities in the UK and Germany have warned critical industries in the private sector that their networks are the targets of foreign intelligence intrusions. In the United States, extensive press reporting has revealed intrusions by foreign intelligence agencies, often attributed to China, aimed at the defense manufacturing and power sectors in particular.

"There are absolutely foreign entities that would definitely conduct [cyber] reconnaissance of our power infrastructure," said Michael Assante chief security officer of the North American Electric Reliability Corporation. "They would be looking to learn, preposition themselves to get a foothold and try to maintain sustained access to computer networks."

Attacks are frequent and their impact is severe

Nearly one-third (29 percent) of those surveyed reported suffering large-scale DDOS attacks multiple times each month, and nearly two thirds (64 percent) of those said such attacks "impacted operations in some way."

Distributed denial of service (DDOS) attacks use networks of infected computers—often owned by individuals or organizations who do not even

know they have been compromised—to bombard target networks with millions of fake requests for information over the Internet. DDOS attacks are conducted by "robot networks"—or "bot-nets"—of computers infected by specially written malicious software, known as malware.

In today's network environment, DDOS attacks are technically easier to detect and tamp down, and most Internet Service Providers (ISPs) offer such mitigation to their clients—for a price.

"Generally ISPs very much have the mentality that we just haul traffic," said Adam Rice, chief security officer of Tata Communications, the world's largest wholesaler of internet service. "If you pay for the [mitigation] service, we'll kill [a DDOS attack] before it gets to you, but otherwise providers tend to watch it go by."

By acting together, he said, the "tier one providers"—who own and operate the backbones of the global Internet—could do much more technically to mitigate such attacks.

The problem, as other experts pointed out, is that such mitigation activities could be complicated by regulatory and contractual concerns, unless the law provided safe harbor provisions for companies intercepting and diverting DDOS traffic. Moreover, providers who operated in more than one national market might face competing or even contradictory legal obligations in different jurisdictions.



Nearly two-thirds of those experiencing large-scale DDOS attacks said their operations had been affected.

Attackers are often anonymous

The attack instructions broadcast to botnets often come from other infected computers, also owned by innocent third parties, with the real authors of the targeting information hidden behind cut-outs and false trails. Botnets can easily be rented from hacker gangs. These factors can make it very difficult to trace the true origin of such DDOS attacks; and the precise identity of those behind the attacks on Georgia and Estonia remains a matter of dispute.

“Knowing something is different from being able to prove it,” said one former U.S. law enforcement official. “Even if you can trace something back to a box, that doesn’t tell you who was sitting behind it.”

The same is doubly true in relation to stealthy infiltration of networks. In the GhostNet case, researchers found spyware—software designed to steal passwords, login information and confidential documents—on computer networks belonging to the office of Tibetan spiritual leader, the Dalai Lama, and blamed the Chinese government. But their attribution was not solely based on a technical trail, but on the fact that data stolen from the compromised networks was later used by Chinese officials.

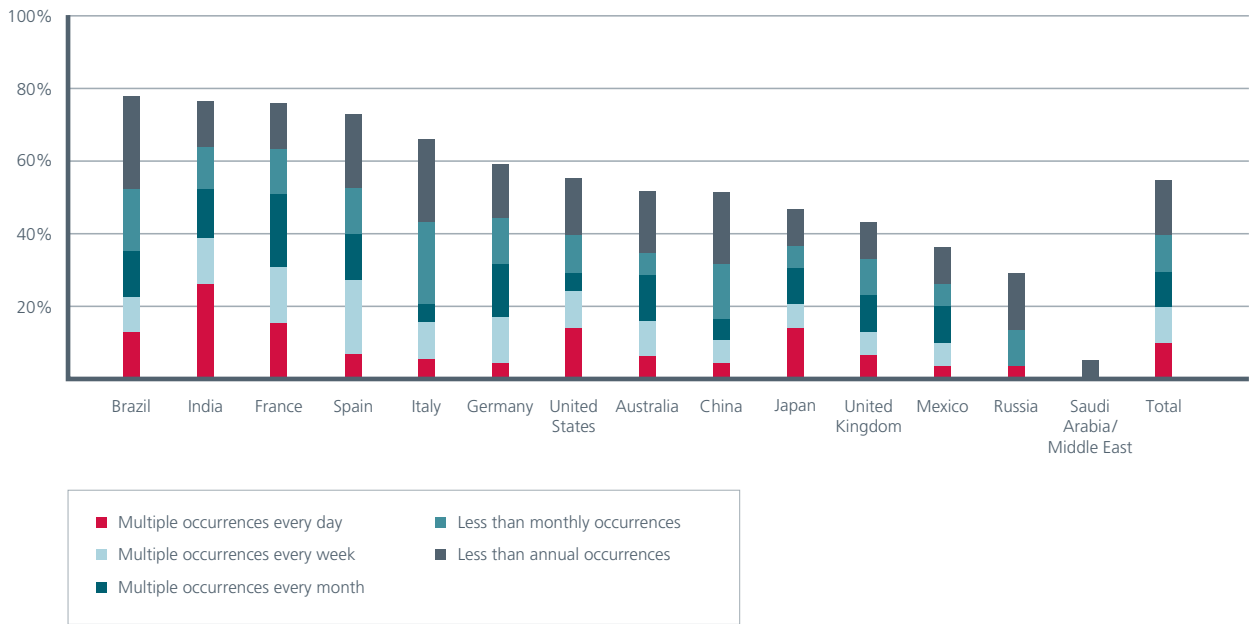
Because of the difficulties inherent in definitively attributing cyberattacks, nation-state attackers continue to enjoy the strategic advantages of “plausible deniability.” But for those charged with defending critical networks, cyber conflict can appear Hobbesian—a “war of all against all.”

DDOS attacks, though widespread, are far from the most common security problem

The most widely reported form of attack was infection with a virus or malware, which 89 percent say they experienced. But victimization rates were also over seventy percent for a wide range of other attacks, including low-level DDOS and vandalism, insider or employee threats, loss or leakage of sensitive data, and phishing or pharming.

More technically sophisticated attacks tended to be more rare than that, although they were still more widespread than large-scale DDOS. More than half (57 percent) of IT executives reported DNS poisoning—where Web traffic is redirected—with nearly half of those reporting multiple monthly occurrences. Roughly the same number had experienced SQL injection attacks—which hackers can use to gain access to back-end data through a public Web site—again with nearly half suffering multiple monthly attacks. Such attacks also tended to have a more significant operational impact on victims’ systems.

Percentage reporting large-scale DDOS attacks, and their frequency



Theft and other monetary motives are common

Sixty percent of those surveyed reported theft-of-service cyberattacks, with nearly one in three reporting multiple attacks every month. Victimization rates were highest in the oil/gas sector, where three quarters of respondents reported theft-of-service attacks. The oil and gas sector also reported the highest rates of stealthy infiltration—71 percent, as opposed to 54 percent of respondents overall, with more than a third reporting multiple infiltrations every month.

In general, however, the variations between victimization rates were wider between countries than between sectors, suggesting that national factors are more significant than sector or industry specific ones in determining attack rates.

Some countries suffer much more frequent cyberattacks than others

In India and France, more than half of executives reported multiple large-scale DDOS attacks every month. Spain and Brazil also had high multiple victimization rates.²

“DDOS attacks are very common in Brazil, as they are everywhere else in the world,” said Achises De Paula, an iDefense Labs analyst based there, adding that ISPs were becoming better at managing them.

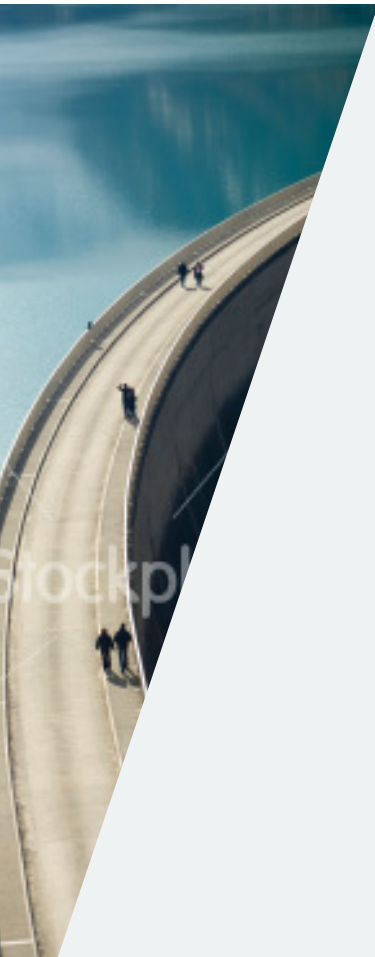
“DDOS attacks are growing in popularity and increasingly cheap and easy to do,” said Rice. “You can rent a botnet to do a DDOS attack... using your credit card within a couple of hours.”

All sectors face DDOS attacks

The sector variations in large-scale DDOS attacks were much smaller than those between countries, perhaps reflecting the greater significance of national as opposed to industry specific factors in determining victimization rates. The most victimized sector was oil and gas, where two thirds of executives report such attacks, with one third reporting multiple attacks a month. The least victimized sectors for this kind of attack were water/sewage, where only 43 percent reported them and transportation (50 percent).

Impact of attacks is severe and varies across sectors

Nearly two-thirds of those experiencing large-scale DDOS attacks reported that these had affected their operations in some way. Such attacks do not just make public web sites inaccessible. They can affect email connectivity, Internet-based telephone systems and other operationally significant functions.



Web of Extortion

One-in-five critical infrastructure entities reported being the victim of extortion through cyberattack or threatened cyberattack within the past two years. This striking data was consistent with the anecdotal accounts of experts from several different countries and sectors; indeed, some suggested the real figure might even higher. Most such cases go unpublicized if not altogether unreported, they said, because of reputational and other concerns by the victim company.

Victimization rates were highest in the power (27 percent) and oil and gas (31 percent) sectors.

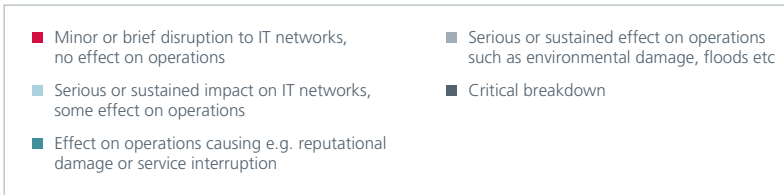
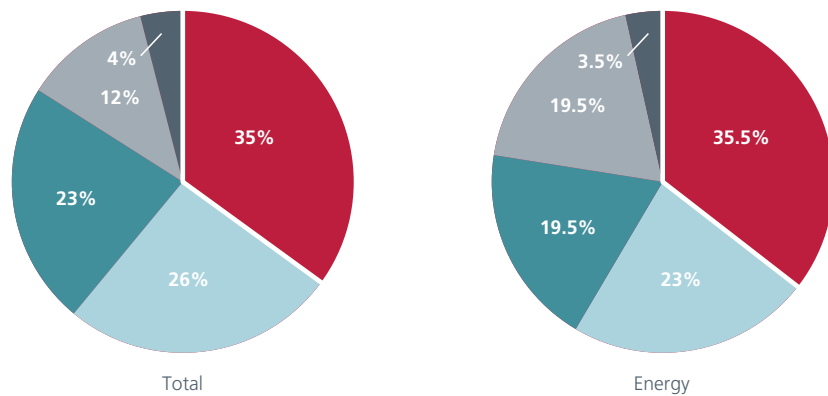
"I am very worried about extortion as it relates specifically to power system interruption," said Assante. He called threats against company networks "lower level" extortion—"the safest way to pull money under the radar and off the books at a level that is not that material." Threats against the infrastructure itself were much more serious. "If you take that to 'hey I can make the lights go out,' then you're talking about a whole

different situation. It's probably a lot higher risk for the extortionist, but you could demand a whole lot more money." In November 2009, there were reports in the U.S. media that two power outages in Brazil, in 2005 and 2007, had been caused by hackers, perhaps as part of an extortion scheme.

In September 2009, Mario Azer, an IT consultant for Long Beach, Calif.-based oil and gas exploration company Pacific Energy Resources pled guilty to tampering with computer systems after a dispute with the firm about future employment and payment. He interfered with specially built industrial control software called a Supervisory Control And Data Acquisition (SCADA) system—in this case one designed to alert operators to leaks or other damage to the miles-long undersea pipelines connecting the company's derricks to the shore.

While the water/sewage sector had a lower rate of victimization (17 percent) the potential impact of extortion schemes is nonetheless felt very keenly in that sector.

Impact of large-scale DDOS attacks

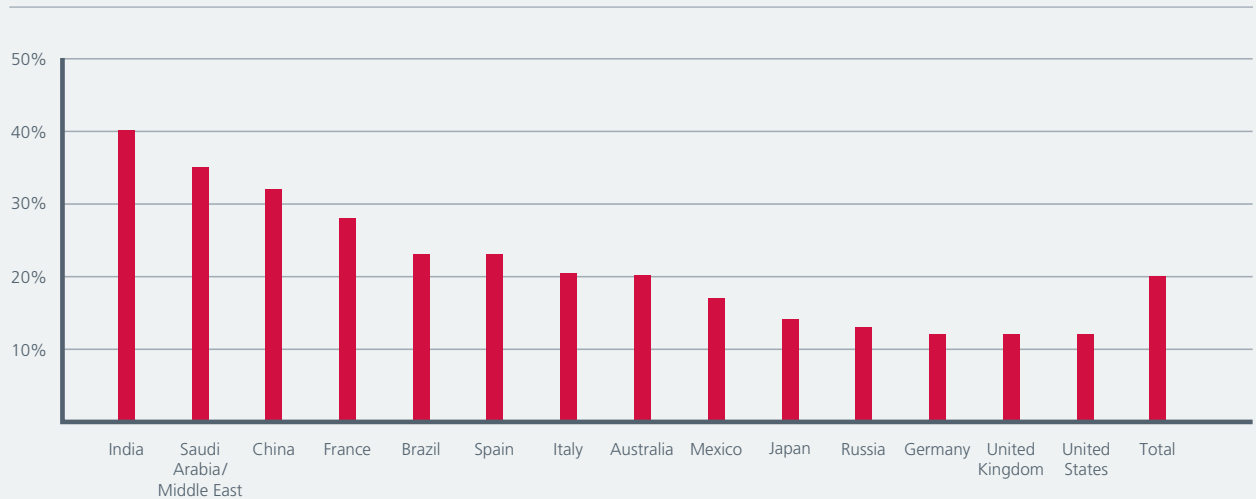


“Clean drinking water is something that the majority of the American population and most of its political leaders take very much for granted, and have done for the last century if not more,” said Aaron Levy of the Association of Metropolitan Water Agencies. “A loss of confidence in the

drinking water supply, studies have shown, could lead to chaotic conditions” in major cities and other population centers.

Extortion was most common in India, Saudi Arabia/Middle East, China and France. It was rarest in the UK and United States.

Percentage reporting extortion using network attack or the threat of it in the past two years



About one-in-six described the impact of large-scale DDOS either as “a serious or sustained effect on operations” or a “critical breakdown.”

These large-scale DDOS attacks had a particularly severe effect in the energy/power and water/sewage sectors.

Other attacks reported as having serious operational impact were stealthy network infiltration, sensitive data leaks or loss, DNS poisoning and SQL injection—all of which had operational consequences for more than 60 percent of victims. For sensitive data leaks and loss, 15 percent said the impact was serious, four percent called it critical.

Executives reported a range of other effects from cyberattacks. The most widely feared non-operational impact was damage to reputation, followed by the exposure of personal information about customers. These two concerns were especially acute in the banking sector.

Follow the money

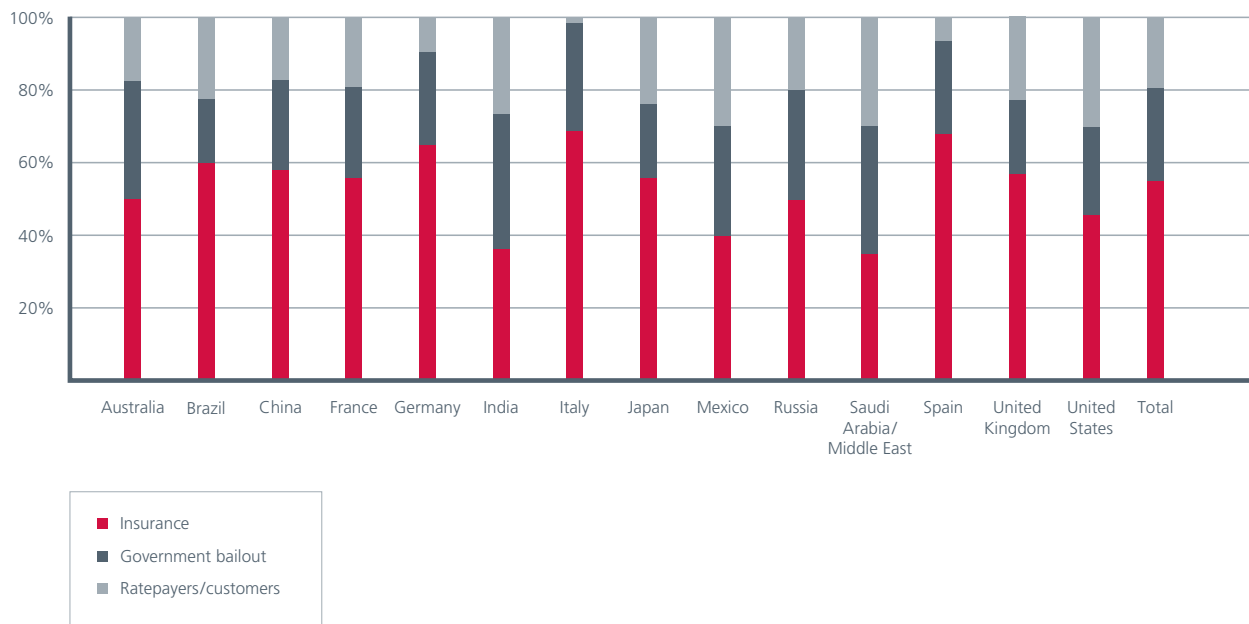
Asked about the most common target of cyberattacks, more than half (56 percent) named financial information. The least common target was password and login information, which was sought in only 21 percent of attacks.

But in the energy/power and oil/gas sectors, attacks were most commonly aimed at computerized operational control systems like SCADA, targeted 55 and 56 percent of the time respectively in those two sectors.

Operational control systems are under attack

Attacks on SCADA systems are especially serious because they can give hackers direct control of operational systems, creating the potential for large scale power outages or man-made environmental disasters. (see page 22)

Who would bear the costs of a major cyber incident in your sector



In 2007, CNN obtained video of a test conducted by scientists at the Idaho National Laboratory, in which an electric generator connected to a SCADA system shook itself almost to pieces after it was fed hacked instructions. The video dramatized the issue of SCADA vulnerabilities in the United States and led to congressional hearings on the cybersecurity of the electricity grid.

Major cyberattacks are costly

Survey data suggests that the costs of the downtime associated with a major cybersecurity incident (“e.g. one that causes severe loss of services for at least 24 hours, loss of life or personal injury, failure of a company”) could be very high.

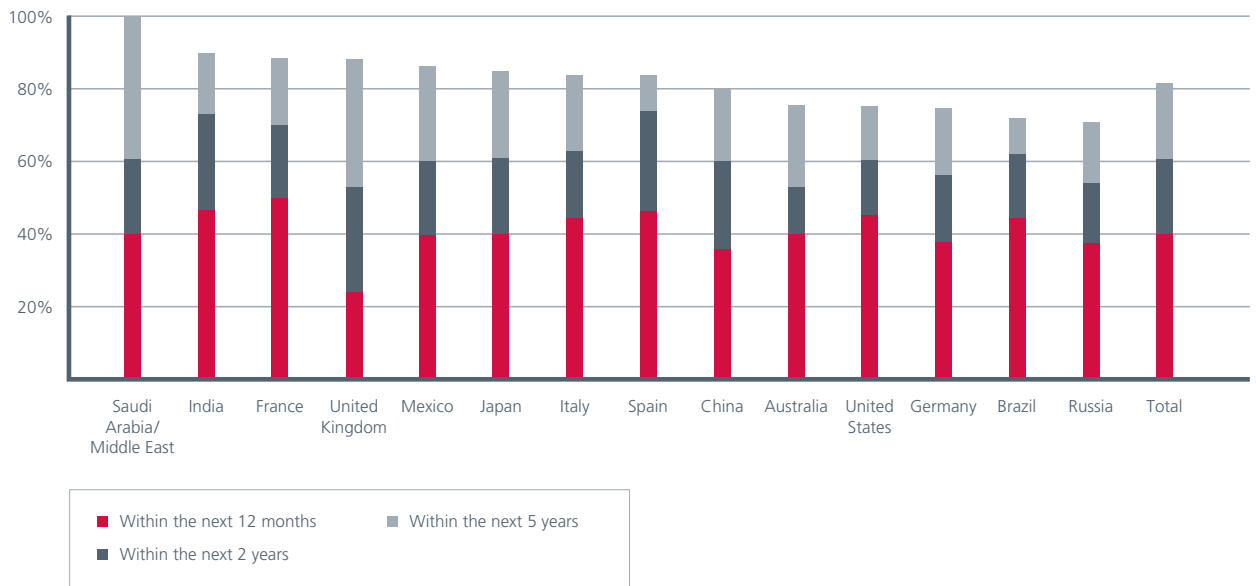
On average, respondents estimated that 24 hours of down time from a major attack would cost their own organization U.S. \$6.3 million. Costs were highest in the oil/gas sector, where the average estimate was U.S. \$8.4 million a day. They were lowest in the government and water/sewage sectors.

Who will pay?

There was considerable variation in expectations about who would have to ultimately bear such costs. More than half of all respondents expected insurance to cover the cost, while nearly one in five said the cost would fall on rate-payers or customers and just over a quarter expecting a government bail-out. Expectations that insurance would defray the cost were highest in Italy, Spain and Germany and lowest in India and Saudi Arabia.

The expectation that costs would be borne by customers were nearly twice as high in the water/sewage sector as among respondents overall (35 percent, as opposed to 19 percent). Where the water sector is an outlier, as here, it is best to bear in mind the small size of the water sector sample. But expectations that the customer would pay were also high in the transportation (24 percent) and telecoms (23 percent) sectors. They were lowest in the oil/gas sector (12 percent).

How long before you expect a major cyber incident affecting critical infrastructure in your country



The average estimated cost of 24 hours of down time from a major cyberattack was U.S. \$6.3 million.

These expectations may turn out to be optimistic. In the future, one expert suggested, they are likely to change—driven by increasing efforts on the part of corporations to limit their liabilities as the costs of cyberattacks mount.

“In Australia [the consumer] has been fortunate to date, in that this has always been someone else’s problem,” said Ajoy Ghosh, a Sydney-based security executive with Logica. “If I’m an individual and I’m the victim of a phishing attack... I know that the bank is going to refund my money... I can see a situation in the future where that’s going to be flipped around and it will be my problem.”

Ghosh, a lecturer in cybercrime at the University of Technology in Sydney, said that as corporations sought to limit their liabilities “the only way they can do that is by making it someone else problem. Sometimes that someone else is going to be the government, sometimes it’s going to be the insurer, but more often than not, I suggest, that someone else is going to be the consumer.”

The risk of cyberattacks is rising

The situation is becoming worse not better. By nearly two to one, those who said the vulnerability of their sector to cyberattacks had increased over the past year outnumbered those who said it had decreased (37 percent, as opposed to 21 percent).

Remarkably, two-fifths of these IT executives expected a major cybersecurity incident (one causing an outage of “at least 24 hours, loss of life or... failure of a company”) in their sector within the next year. All but 20 percent expected such an incident within five years. This pessimism was particularly marked in the countries already experiencing the highest levels of serious attacks.

Responding to the Threat— Resources and Preparedness





Cuts in security resources as a result of the recession are widespread. Making the business case for cybersecurity remains tough.

Most IT executives say that their resources for network protection are adequate, though there is a lot of variation in the level of satisfaction from country to country. But cuts in those resources as a result of prevailing economic conditions are also widespread. Making the business case for cybersecurity remains a challenge.

Confidence about resources does not always translate into confidence about preparedness. About a third of those surveyed say their sector is unprepared to deal with major attacks or stealthy infiltrations by high-level adversaries. And Europeans in particular have low levels of confidence in the capacity of their banking infrastructure to operate in the event of a major cyberattack.

Resources are generally considered adequate

IT executives generally believed they had adequate resources to protect their organization's computer networks. Nearly two-thirds of the surveyed said their resources were either "completely" or "mostly" adequate. Just over a third said their resources were "inadequate" or only "somewhat adequate."

Some countries and sectors were less satisfied than others

The number who said resources were adequate was lowest in Italy, Japan and Saudi Arabia; and highest in Germany, the UK, and Australia. Banking respondents were generally the most satisfied with their resources, transportation/mass transit the least.

Recession-driven cuts in resources are widespread and in some cases deep

Two-thirds of the IT executives surveyed said there had been cuts in the security resources available to them as a result of the recession.

One in four said those cuts had reduced their resources by 15 percent or more. Energy and oil/gas were the sectors with the most widespread cuts, with up to three-quarters of respondents reporting reductions. Cuts were most widespread in India, Spain, France and Mexico; and least widespread in Australia.

Security is a key factor in investment decisions

Even in a recession, security is still the top factor in making IT investment and policy decisions. In making IT investment and policy decisions, 92 percent said security was either "vital" or "very important." Nearly as many, 91 percent, said the same of reliability. The other two factors the survey asked about, efficiency and availability, were said to be vital or very important by three quarters of the executives.

Executives in China and the United States were the most likely to call security "vital."

Business incentives for cybersecurity: the three-legged stool

Overall, cost was most frequently cited as "the biggest obstacle to ensuring the security of critical networks," followed by "Lack of awareness of the extent of the risk."

But in the water/sewage and oil/gas sectors, those obstacles were reversed in significance, with lack of awareness being most frequently cited, ahead of cost. Security specialists from several sectors said that making the business case for cybersecurity remains a major challenge, because management often does not understand either the scale of the threat or the requirements for a solution.

"The number one barrier I think is the security folks who haven't been able to communicate the urgency well enough and they haven't actually been able to persuade the decision makers of the reality of the threat," said one security specialist. He added that in part this was because security had not yet become a significant market differentiator for critical industries.

Experts generally agreed that awareness of cybersecurity issues in the United States and elsewhere had grown since the September 11 terrorist attacks, with increasing emphasis from governments on hardening critical infrastructure. But they said there was a long way to go.

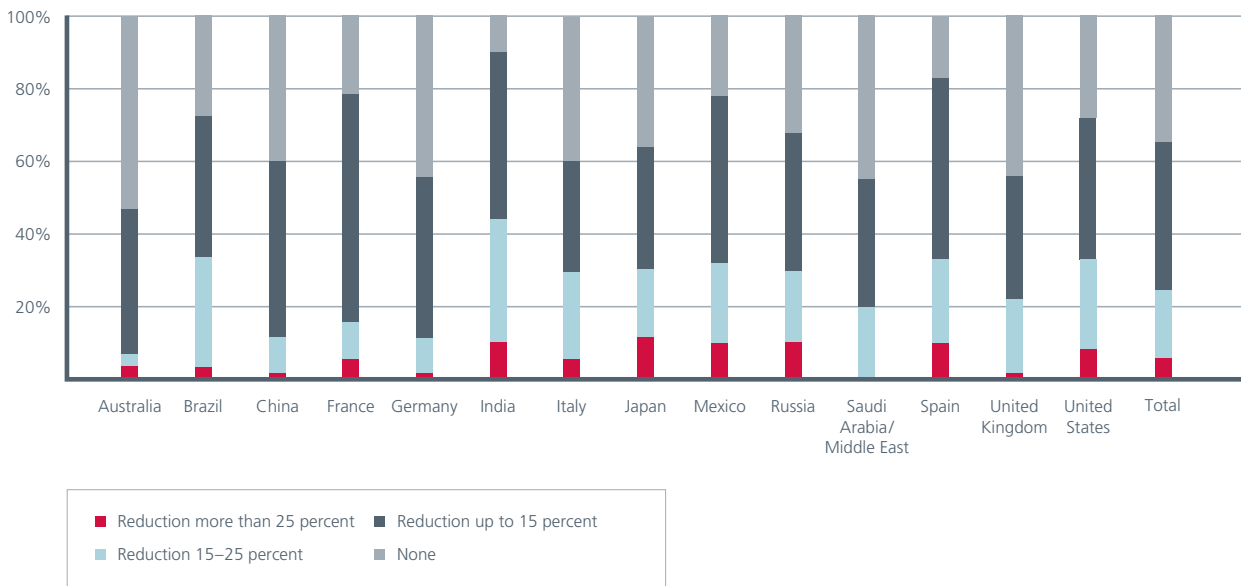
"Cybersecurity is really just emerging as something that utility managers and their security managers are keeping their eyes on," said Aaron Levy of the Association of Metropolitan Water Agencies. "Everyone is still playing a little bit of catch-up," added a transportation sector specialist.

Unfortunately, experience remains the best teacher, which means that it often takes a serious attack to convince management of the reality of the threat and the need to protect against it. "Companies that are handling their cybersecurity well are typically the ones who have experienced adverse events in the past," said the specialist.

On the other hand, the CSO of one of the world's largest telecommunications and internet providers, told us that customers had begun to focus more



Cuts in security resources caused by the recent recession



on security—making it a market differentiator. “It’s totally customer driven,” said Adam Rice of Tata. “Companies no longer look around once they’ve decided to close the deal and say ‘oh by the way, what about security?’ It’s upfront, it’s an absolute requirement... our customers want to see it. They want to get on calls and ask tough questions, they want to visit data centers, they want the right to come in unannounced... customers will drop the requirements on us and we have to meet them.”

Even so, making the business case for security could be a challenge. “No one wants to pay their insurance bill until the building burns down,” said Rice. “The best way a CSO can demonstrate their usefulness to the rest of the executive team is by identifying... how security issues can pose a risk to revenue... spelling out how a dollar spent today can potentially save millions tomorrow.”

A lot depends on your position within the organization. “Typically, if your CSO does not report to the CEO, he is probably too deep within the organization.”

More than three quarters, 77 percent, of the IT and security executives surveyed reported their company had a chief information security officer. Nearly half, 46 percent, said their CISO reported directly to the chief executive officer.

Creating incentives for better security was also an area where several experts said there might be a role for government. Although the effects of regulation are complex (and are examined in more detail in Chapter 4), some saw other ways in which governmental action could change security incentives.

“Cyber is a three-legged stool,” said retired Gen. Michael Hayden, adding the three legs were “ease-of-use, security and privacy... To date, almost all of our creative energies have been put into ease of use.”

“Like any three-legged stool, if you don’t have all three legs, what you have is firewood,” he said, adding that the paradigm which prioritized ease-of-use over the other two legs had to change.



Confidence in preparedness is variable

Nearly a third of the IT executives surveyed said their own sector was either “not at all prepared” or “not very prepared” to deal with attacks or infiltration by high-level adversaries. Among those who had actually experienced such attacks, this lack of confidence rises to 41 percent.

But there were significant variations between nations. In Saudi Arabia, a remarkable 90 percent said that their sector was unprepared (either “not at all prepared” or “not very prepared”). In most countries, those who had suffered high-level attacks tended to be more pessimistic about preparedness, with 68 percent of Indian victims and 75 percent of Mexican victims saying their sector was unprepared for them.

The countries where executives were the most confident about their preparedness for high-level attacks were Germany (78 percent) and the UK (64 percent).

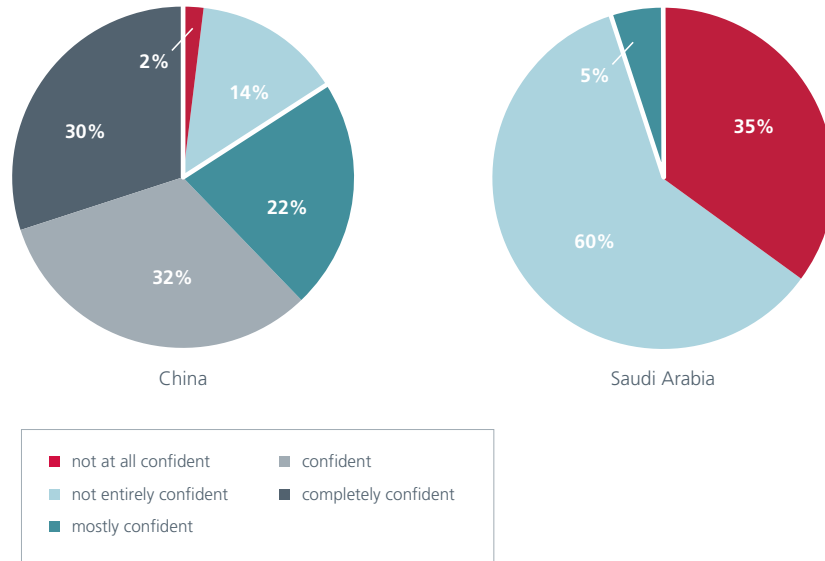
Beyond high-level DDOS, executives generally rated their sectors as better prepared against other forms of attack, with roughly only one in four saying their own sector was unprepared against them.

Across the whole range of threats, those in the United States, the UK and Australia consistently ranked their sectors the highest for preparedness. All of these countries have high-profile programs of government outreach to critical infrastructure owners and operators.

Doubts about whether banking and phone systems can withstand attack

IT executives were also doubtful about the ability of their own critical infrastructure providers to offer reliable service in the event of a major cyberattack. Thirty percent lacked confidence that their bank or other financial service provider could. And 31 percent had the same doubts about their telecom provider. Confidence in the resilience of the banking system was lowest in some European countries: Italy, France and Spain.

Confidence that government services could withstand a major cyberattack

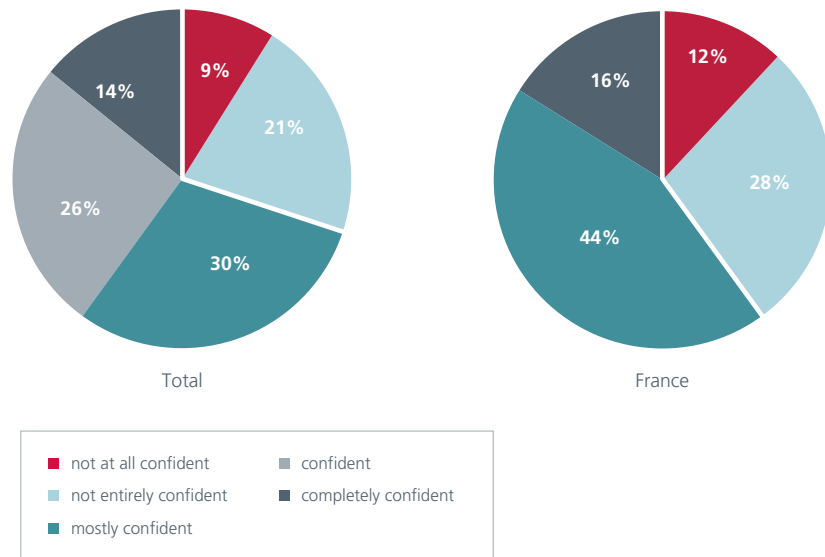



During the DDOS attacks against Estonia in 2007, many of the country’s banks had their Web sites knocked off-line, though they said afterwards that operational systems were not compromised. Security specialists from different sectors and countries agreed that banking and financial services tend to have higher levels of security. But they also have the “Willy Sutton problem”—when asked why he robbed banks, Sutton apocryphally replied

“because that’s where the money is”— financially motivated cyberattackers will always be drawn to that sector.

The level of confidence about government services was higher than for most sectors. Even so, only 37 percent of respondents were confident their government could continue to deliver services in the face of a major cyberattack. Confidence in government was lowest in Saudi Arabia, highest in China.

Confidence that banking and financial services could withstand a major cyberattack



A photograph of a busy office hallway with several people in business attire walking. The image is intentionally blurred to convey a sense of motion and activity. The background features a wall with large windows and a modern architectural style.

Countering the Threat— Security Measures



Basic, key security measures are not widely adopted.

IT and security executives were asked a series of detailed questions about more than two dozen different security measures—technologies, policies and procedures—and how they were used.

Those with responsibility for their organization’s SCADA or Industrial Control Systems (ICS) were asked a similar series of questions about the measures employed on those networks. The data about SCADA/ ICS, although based on a smaller number of respondents, is striking. More than three quarters of those with responsibilities for such systems reported that they were connected to the Internet or some other IP network, and just under half of those connected admitted that this created an “unresolved security issue.”

The other responses, taken question by question, reveal that some basic, key security measures are not widely adopted.

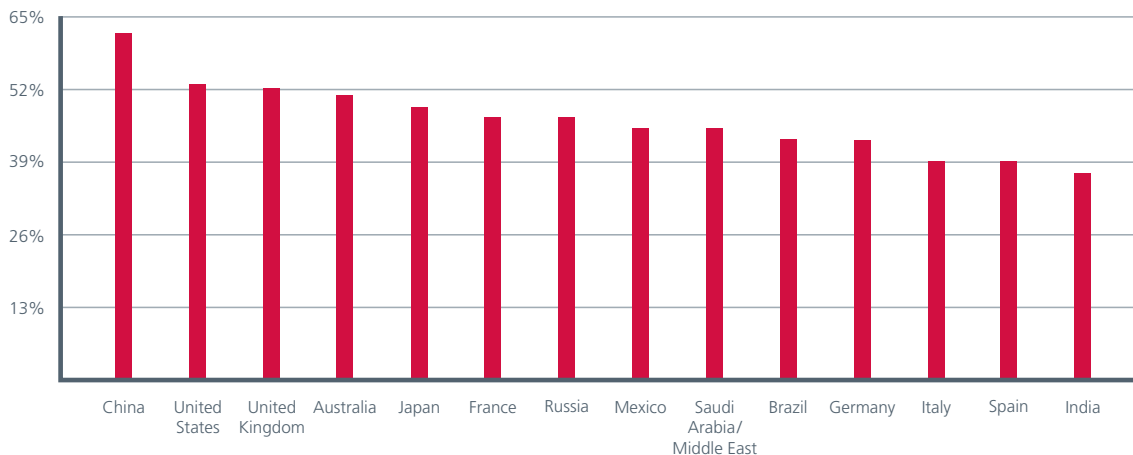
And amalgamating this data shows which countries and sectors have the highest and lowest adoption rate of these security measures overall. This is not necessarily a measure of how “good” or “bad” security is in a sector or country, but it does offer insights into security practices that are not on the subjective self-assessment of the respondents, but on the objective rate at which key security measures are deployed.

Using this measure, China had the highest security adoption rate overall—62 percent—well ahead of the United States, the UK and Australia, the next highest rated countries, with 50–53 percent.

Italy, Spain and India had the lowest security adoption rates—all under 40 percent. The remaining countries—Japan, Russia, France, Saudi Arabia, Mexico, Brazil and Germany—were all in the 40–49 percent range.

The sectors with the highest security adoption rates were banking and energy. Water/sewage had the lowest rate of any sector.

Security measure adoption rates reported by respondents



The Security Measure Adoption Rate (SMAR)

IT and security executives were asked about 27 different security measures: ten security technologies, six security policies, five different ways of using encryption, and six different modes of required authentication. The SMAR essentially quantifies how often executives said “yes” when asked if they employed a particular measure.

Every organization has its own security strategy, and different uses can be made of many of the measures executives were asked about. For this reason the SMAR cannot necessarily be taken as a gauge of how “good” or “bad” security is in a given sector or country. But it does enable comparative judgments about the rate at which different sectors and nations have adopted key security measures. It is a rough measure, because every security technology, practice or policy is given the same weight, no matter how effective it is, but it is objective.

Chinese executives reported far and away the highest security adoption rate—62 percent

They reported higher levels of adoption than any other country of every kind of security measure. The United States, with a 53 percent adoption rate, and Australia and the UK, with 51 and 52 percent respectively, were the countries with the next highest rates after China.

Italy, Spain and India had the lowest overall adoption rates—all fewer than 40 percent. The remaining

countries—Japan, Russia, France, Saudi Arabia, Mexico, Brazil and Germany—were all in the 40–49 percent range.

Do higher security adoption levels reduce the risk of successful attacks?

This is a critical question, but the answers provided by the survey are mixed. On the one hand, China, with its high rate of security measure adoption, does have a victimization rate that is lower than countries at the bottom of the security adoption rate scale like India. Other data also suggest that nations with lower adoption rates may suffer in various ways. McAfee’s global threat intelligence division, for instance, monitors malicious electronic traffic from compromised computers recruited into botnets after becoming infected. According to that data, India, the nation with the lowest rate of security measure adoption, tops the charts for malicious traffic in Asia—producing more than Russia and China combined.

On the other hand, China’s overall security record is not noticeably better than the record of many other countries with much lower security adoption rates. China is not notably free from high-level attacks, nor do Chinese respondents rate themselves as being much better prepared than other nations.

Some key measures are not widely adopted

The least widely adopted security technology was application white-listing, implemented only by fewer than one-fifth (19 percent) of organizations on both SCADA/ICS and IT networks. Other more

China vs. India

What explains the enormous difference between security measure adoption rates in these two Asian powers? Both see themselves as heavily regulated. More executives in India than any other country reported that their cybersecurity was subject to law or regulation, 97 percent, while China was the second most regulated country, tied with Germany at 92 percent. But attitudes toward government varied substantially. In China, 91 percent of those regulated said they had changed company procedures as a result, whereas in India, only 66 percent said they had made changes. And India reported among the lowest levels of participation in government critical infrastructure partnership organizations, while China had the highest level.

Executives in China also had much higher levels of confidence in the capabilities of their government to deter and prevent cyberattacks. McAfee global threat intelligence data suggests that India has recently replaced China (and Russia and Romania) as the richest hunting ground for hackers bent on recruiting infected computers for botnets, another possible result of the disparity between the two countries' security adoption rates.



Chinese executives reported far and away the highest security adoption rate.

advanced security technologies like Security Information and Event Management systems, and role and anomaly detection tools, were employed by 43 and 40 percent respectively.

Experts said that the benefits of some newer tools might not be well understood in the marketplace, or might be only suitable for larger enterprises.

But some much more basic measures were not widely implemented either. Only 57 percent of executives overall said their organization patched and updated software on a regular schedule. Regular patching was most widely reported in Saudi Arabia (80 percent) Russia (77 percent) Australia (73 percent) and least common in Brazil (37 percent).

And only one third of executives reported that their organization had policies "that restrict or ban the use of USB sticks or other removable media." Apart from the risk that data may be downloaded, stolen and smuggled off the premises, such media—even when used without ill intent—can easily spread viruses and other malware, even across systems that are firewall-protected. Bans on USB sticks and other such media were most widely adopted in Saudi Arabia (65 percent) and Russia (50 percent). They were most rare in Spain (13 percent) and Brazil (20 percent).

Other measures are more common

The most widely adopted security measure overall was the use of firewalls between private and public networks, which 77 percent reported using (65 percent for SCADA or ICS systems).

Threat-monitoring intelligence services are most widely adopted in India (57 percent) China (54 percent) and Japan (54 percent), while they are used least in Saudi Arabia (20 percent) Russia (23 percent) and Italy (20 percent).

Wide variations in the use of encryption

As with almost all adoption rates, China led in the use of encryption. The one exception was the use of encryption to protect data on CDs or other removable media, where China's 48 percent adoption rate trailed the 56 percent rate in the United States and the 54 percent rate in Japan and the UK. India had lower than average adoption rates for five out of six uses of encryption. Italy and Spain also had generally below average adoption rates for encryption.

Water/sewage sector lags in adoption rates

The sectors with the highest overall adoption rates were banking/financial services and energy, each with 50 percent. Water/sewage had the lowest sector rate, 38 percent. Other sectors were all in the 40-plus range.

The water/sewage sector also had the lowest adoption rate for security measures protecting their SCADA/ICS systems, perhaps because the sector also had the lowest levels of SCADA connections to IP networks, with only 55 percent reporting such connections, in contrast to 76 percent overall.

When considering this data, the small number of water sector executives amongst those with SCADA/ICS systems responsibilities—only 11 out of 143—needs to be noted.



Eighty percent reported SCADA systems were connected to IP networks or the Internet, despite the risks involved.



SCADA security

We also created a SMAR scale for SCADA and ICS systems, based on a list of 16 security and authentication measures those with responsibilities for such systems were asked about. (Caution is required in interpreting these figures because of the smaller numbers of respondents. Only 143 out of 600 had SCADA responsibilities and were asked about their organizations' SCADA systems.)

China again led the field, with a security measure adoption rate for SCADA/ICS security measures of 74 percent, way ahead of second-place Australia at 57 percent, and Brazil, third with 54 percent. The range of security adoption rates between countries is particularly striking. Adoption rates for SCADA/ICS measures were lowest in India and Spain at 29 percent each and the UK at 31 percent—meaning that Chinese SCADA/ICS operators have adopted nearly three times as many key security measures as Indian and Spanish operators.

In the middle were the United States and Japan with rates of 50 percent, followed by France, Russia, Germany, and Saudi Arabia in the 40-plus percent range and then by Italy and Mexico with 38 and 35 percent respectively.

Some tools like application white listing and SIEM appeared to be more widely adopted in SCADA/ICS systems than in IT networks.

Executives generally reported very high levels of connection of SCADA systems to IP networks or the Internet, despite widespread acknowledgment about the risks involved.

Seventy-six percent of respondents with SCADA/ICS responsibilities said their networks were “connected to an IP network or the Internet.” Nearly half of those connected, 47 percent, admitted that the connection created an “unresolved security issue.”

Connections to IP networks pose a vulnerability because they might allow unauthorized users access to the systems at the heart of critical infrastructure, said one veteran IT security executive. “The original SCADA design generally didn’t assume that the control systems would be exposed on networks where untrusted people had at least some level of access to them.” Much SCADA software was written “quite some time ago and has not been modified since.” The systems “are not [running] on the newest platforms, so they have those vulnerabilities that have been discovered over time.”

Because SCADA systems often combine hardware and software, they cannot be updated like regular software can be and replacing them is “hugely complex and hugely expensive,” said the veteran. There is “no mechanism for revisiting the system and changing them once vulnerabilities are discovered.”



A cybersecurity specialist from the power sector said that SCADA systems were “developed as engineering supported environments” with few security features. They are “typically open and difficult to secure.”

Some experts said SCADA/ICS networks should not be connected to the Internet, period. “Control systems should be their own dedicated infrastructure and should not be connected to the open internet,” said one transportation sector specialist, adding that he thought in some cases the reason ICS networks are connected to the Internet “is simple convenience.”

The Conficker worm, which spread on the Internet, has been a wake-up call in some respects, added the power sector specialist. It “got into places that raised real concerns as to how it got there.”

But experts also said there was a growing awareness of the vulnerabilities of SCADA systems, which was borne out by the survey data.

“Five years ago, realistically,” said the transportation specialist, “If you went into any of the key organizations in this sector or in most other sectors and talked to the people responsible for cybersecurity... they would have had no knowledge of the control systems that in many cases

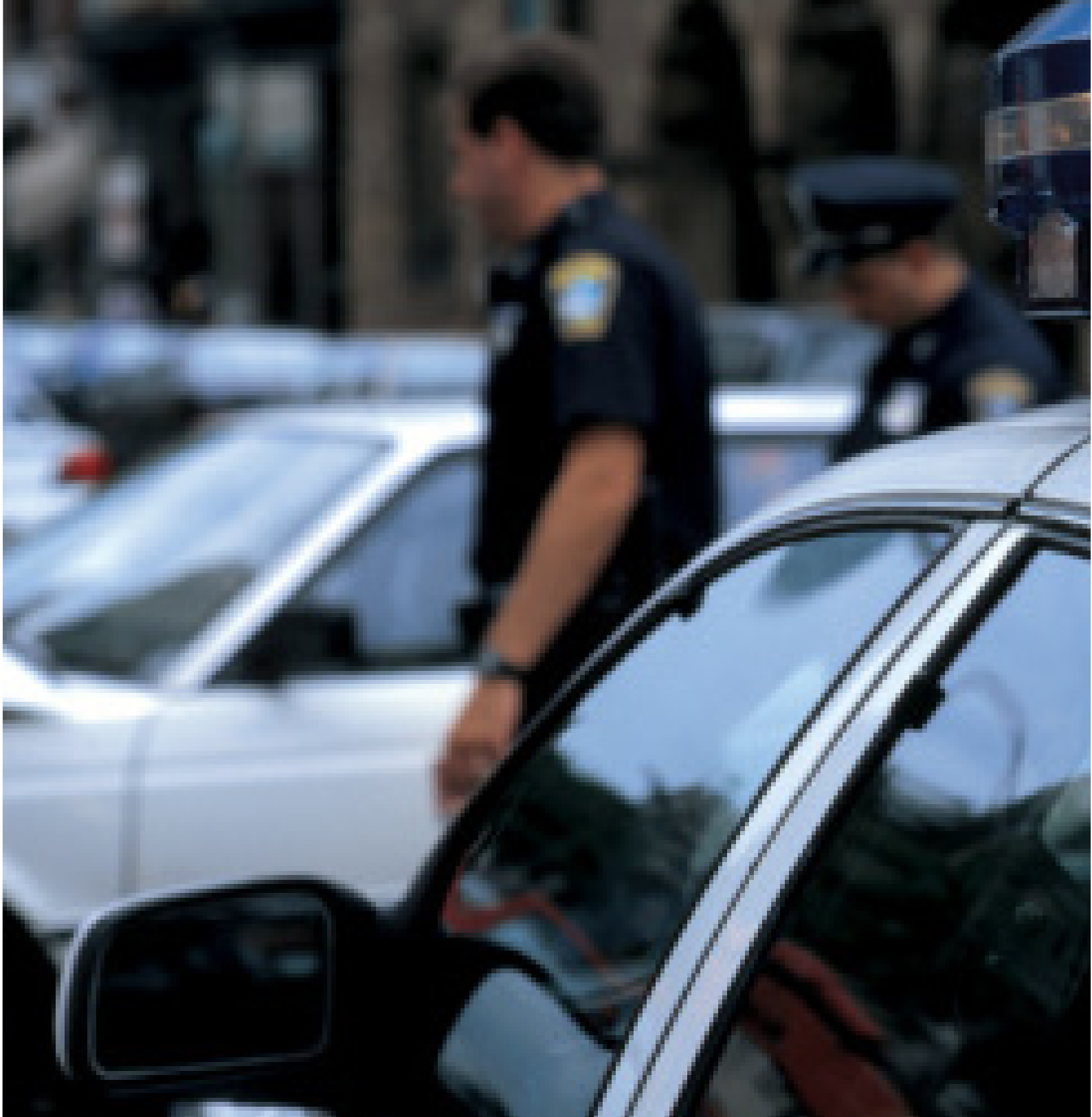
that they even existed, what they were, how they worked, because they were not within the purview of the CIOs of these organizations and the cybersecurity staff. They belonged to the operational staff and there was absolutely no attention being paid to cybersecurity.”

“It is probably safe to say,” the specialist concluded, “that everyone is still playing a little bit of catch-up.”

Ninety-two percent of the executives with responsibility for SCADA systems reported monitoring them in some way. The most widely adopted measures were network behavior analysis tools (62 percent overall), with China (100 percent), the United Kingdom (78 percent), and Mexico (75 percent) the top adopters of such tools. Fifty-nine percent of respondents used audit logs, with Germany (90 percent) and China (82 percent) at the top in employing that measure.

Only eight percent said they did not monitor new IP connections to SCADA/ICS systems.

The "State of Nature" and the Role of Government





IT executives rank the United States as the country “of greatest concern” in the context of foreign cyber attacks.

Cyberspace today most resembles what Hobbes called a state of nature—a “war of every man against every man.” Hobbes thought that only government and law could end that war. But in cyberspace, the role of government is more complicated. Globally, a majority of critical infrastructure is in the hands of private companies, which often operate in more than one country. For these companies, governments are partners; they are regulators and policemen; they are owners, contractors and customers; but they are also seen as aggressors, infiltrators and adversaries.

Even when governments assume the role of defender, seeking to prevent attacks and improve security, many IT and security executives are skeptical about their ability to deter or protect against cyberattacks—although attitudes vary from country to country.

One area where government is seen as having a generally positive impact is in regulation. Audit and enforcement rates and the impact of regulation on security vary widely from country to country, as do perceptions about its effectiveness.

Many governments have sponsored cybersecurity cooperation among owners and operators of critical infrastructure, but widely varying levels of participation are reported.

Chinese executives report a uniquely close level of cooperation with government, as well as high levels of regulation by, and confidence in, government. These figures are striking; they identify China as a leader in government engagement with industry.

IT and security executives across the world show great ambivalence toward the United States. It is the nation most often cited as a model in dealing with cybersecurity. At the same time, executives from many nations, including many U.S. allies, rank the United States as the country “of greatest concern” in the context of foreign cyberattacks, just ahead of China.

Percentage believing current law in their country is inadequate against cyberattackers



Doubts about the ability of government and law to deter attackers

More than half of all the executives surveyed thought their nation's laws were inadequate to deter cyberattacks. More than three quarters of Russians held that view, as did large majorities in Mexico and Brazil. Germans had the most faith in their national laws as a deterrent, followed by France and the United States.

There were also doubts in some of those same countries about the capabilities of governments to prevent and deter attacks. A startling 45 percent believed their governments were either "not very" or "not at all" capable of preventing and deterring cyberattacks. In countries like Brazil and Italy, two-thirds or more thought that their governments were either "not very" or "not at all" capable. Mexico, Saudi Arabia, Germany and Spain also had majorities with negative views about their government's capabilities. In the United States, in contrast, only 27 percent of executives deemed the government not capable or not very capable; in China, the "no confidence" vote was almost as low at 30 percent.

"Right now, the sheriff isn't there," said retired Gen. Michael Hayden, who recently ended a long career as a senior U.S. intelligence official as the director of the CIA, saying cyberspace was like the Wild West of legend. "Everybody has to defend themselves, so everyone's carrying a gun." But in the cyber domain that was like expecting each citizen to organize their own national defense. "You wouldn't go to a post office and ask them how they're tending to their own ballistic missile defense... but that is the equivalent of the current set-up in cybersecurity," Hayden said.

Most believe that government regulation is improving security

Many experts agreed that governments need to do more to improve cybersecurity for critical infrastructure, but the record so far is decidedly mixed—there are many different approaches, their impact is uneven, and IT executives in different countries viewed them with widely variable enthusiasm.

Overall, 86 percent of executive reported that their cybersecurity was in some way subject to law or government regulation. Nearly three-quarters, 74 percent, said their organization had "implemented new policies, procedures, best



A solid majority of IT executives believe regulation and/or legislation has improved cybersecurity.

practices or technical measures” as a result of laws or regulation. There was considerable national variation, and an outlier at either end—91 percent in China had changed policies because of government rules, compared to 56 percent in Spain. In the middle, India, Germany, Italy and Australia all had less than 70 percent saying they had changed procedures.

Forty two percent said that government regulation either had “no significant effect” or actually “diverted resources from improving security”—as opposed to 58 percent who believed that it had “sharpened your policy and improved security.” Countries with a wide variety of national approaches—Brazil, Spain, China, Mexico, Germany and Japan—all had between 60 and 70 percent agreeing that regulation had improved security. Doubts were most widespread in Italy and Australia, where majorities questioned the value of their government’s regulatory regime.

Confidence in the efficacy of regulation was notably low in the water sector, where only 24 percent agreed it improved security. Again, where water is an outlier, the small number of respondents from that sector is worth bearing in mind.

Participation and partnership

Government-sponsored cybersecurity cooperation varies widely among owners and operators of critical infrastructure.

Participation in government-led partnership initiatives is generally low. When asked how they were involved in developing laws or regulations, about a third (35 percent) of executives said their organization was involved in a government-private sector partnership organization. Participation was more widespread in more horizontal organizations like industry information-sharing associations where more than half (53 percent) said they were members.

But participation varied widely between countries. It was highest in China, where 61 percent of executives said they belonged to a government partnership organization. Participation rates were lowest in Brazil (22 percent), and below thirty percent in Japan, Germany, Italy, India and Spain, as well.

Participation rates may not, however, be a good guide to the success of such initiatives. Even in the United States, where participation in partnership bodies, at 42 percent, is relatively high, interview data suggests that well-documented industry concerns persist about information-sharing being a one-way street.

China is a leader in government engagement with industry

Overall, just under half, 49 percent, of IT and security executives reported being audited by a government agency for compliance with cybersecurity laws or regulations. But there were large variations between auditing rates in different countries. Rates were far and away the highest in China (83 percent) and next highest in Saudi Arabia (73 percent). Brazil, Australia and France all reported audit levels above 50 percent. Rates of audit were lowest in Russia (30 percent) and Spain (32 percent).

Chinese executives also reported a high level of regulatory and legislative activity by government, with 92 percent saying they were subject to it, tied with Germany as the second highest rate for any country except India, 97 percent.

The country where executives reported the lowest levels of regulatory activity were the United States,

where 72 percent of executives said they were subject to regulation of their cybersecurity, compared to 86 percent overall.

The United States is seen as a model

Perhaps for this reason, IT and security executives most frequently identified the United States as the one country other than their own that they looked to as a model for cybersecurity, with 44 percent seeing the United States in that light. The next most popular national models are Germany (22 percent) and the UK (18 percent). The U.S. model was especially salient in China (78 percent) and Mexico (72 percent). Its popularity was lowest in Germany (31 percent).

Interview data suggested that the salience of the U.S. model may have more to do with the amount of attention the press and high-profile officials have paid to U.S. efforts in the area than to the way the U.S. government is set up to deal with the issue—few nations seem to be emulating the United States in this regard.

Sources of doubt about the value of regulation

There is clearly widespread concern among executives about the impact of regulation and legislation. This is perhaps unsurprising; using survey responses to determine attitudes to regulation can be problematic. Few business executives ask for more regulation. But several key points emerged.

Interviewees identified three areas of particular concern:

- Lack of faith in the understanding officials have about the way a sector works.
- The possibility that clumsy regulation can “level-down” security in very diverse sectors.
- The risk that mandatory disclosure of security incidents—for example the compromise of personal data—can drive policy and resources in counter-productive directions.

Doubts are notably widespread in the water/sewage sector, where a massive 77 percent said law and regulation had either “diverted resources from

improving security” or had no effect. Executives in the sector also had the lowest level of confidence in their government’s capabilities to prevent or deter cyberattacks.

One U.S. security specialist from the water/sewage sector said that regulatory demands were felt very acutely, especially by smaller concerns in a very diverse sector. “Our guys on the ground are getting into this... ‘feed the beast’ scenario”—chasing discrete regulatory requirements rather than planning for security in a coordinated fashion. “If you’re trying to keep a bunch of masters happy, that’s what drives people crazy. It eats up resources, and it really leaves it to the utility head [to decide] about how they’re going to manage risk.”

The specialist said he and his colleagues “often feel like we’re like the little step-child in the room,” at federal security forums where all the sectors were represented. “We often don’t get the same amount of respect, not on a personal level, but on a tactical and strategic level, that the other sectors get,” the specialist explained.

Percentage reporting auditing by government agencies pursuant to law and/or regulations



But doubts about the value of regulation aren't confined to the water/sewage sector, and interview data suggests that the doubts are driven by more widespread concerns.

"Here in the U.S. there is a lack of confidence in the government's knowledge of what should be done and a lack of knowledge [on the part of the government] of the operation of the various infrastructures," said one transportation sector security specialist. He said there was "substantial worry that regulation is a lot of useless activity at great cost, that provides little to no security."

Experts also expressed concern that in sectors where the operator base is very diverse, regulation, especially if applied as a blunt instrument can inadvertently "flatten" standards. Setting one standard for a diverse sector can improve the security of some players but set a floor which other, more sophisticated enterprises could easily climb above, but now see less incentive to. "In some cases I've heard of organizations and entities that have pulled back how they're managing security in the enterprise to meet specifically what the requirement said," according to one electricity/power sector security specialist.

There is concern that much regulation is "a lot of useless activity at great cost, that provides little to no security."

Executives said that, apart from operational failures, the consequence they most feared from a cyberattack was reputational damage. Anecdotal evidence suggests that laws requiring disclosure of certain security incidents might be driving companies to make investment and policy decisions that will reduce the number of reportable incidents, rather than strengthening the overall security of the enterprise.

In Japan, for example, one official noted that requirements to report information-security accidents to government authorities had given rise to complaints that "there are times [when] the administrative requirements for the person in charge of security outweigh the [seriousness of the] threat" of such incidents.

But the United States was also seen as one of the countries most vulnerable to cyberattack

Fifty percent of IT and security executives also identified the United States as one of the three countries “most vulnerable to critical infrastructure cyberattack in your sector”—ahead of any other country. China was the second most frequently named, (34 percent), followed by Russia (27 percent).

Perceptions of U.S. vulnerability were especially widespread in China (where 80 percent listed it as one of the three most vulnerable nations), Mexico (73 percent), and Brazil and Russia (70 percent each).

China was seen as especially vulnerable by executives based in neighboring regions—with respondents from India (57 percent) Japan (56 percent) and Australia (43 percent) more likely than average to name it in the top three vulnerable nations.

Some experts suggested that the U.S. was seen as more vulnerable because it was more advanced—and more reliant than almost any other nation on computer networks. But others cautioned that U.S. vulnerability in this regard is not unique and can easily be overstated.

The United States and China are both seen as likely attackers in the cyber war

As noted in chapter one, a hefty majority of IT and security executives surveyed believe that foreign governments have already been involved in network attacks on their sector. When they were asked which country “you worry is of greatest concern in the context of network attacks against your country/sector,” 36 percent named the United States and 33 percent China—more than any other countries on a list of six (respondents were also offered the chance to specify a different answer). The next most frequently cited was Russia, a distant third at just 12 percent. None of the other three, the UK, France and Germany, topped six percent.

Different sectors tended to worry about different countries as potential attackers. Among executives in the government sector, for instance, China surpassed the United States as the biggest worry. Energy company executives worried most about Russia, while China and the United States ran neck and neck in the telecom sector.

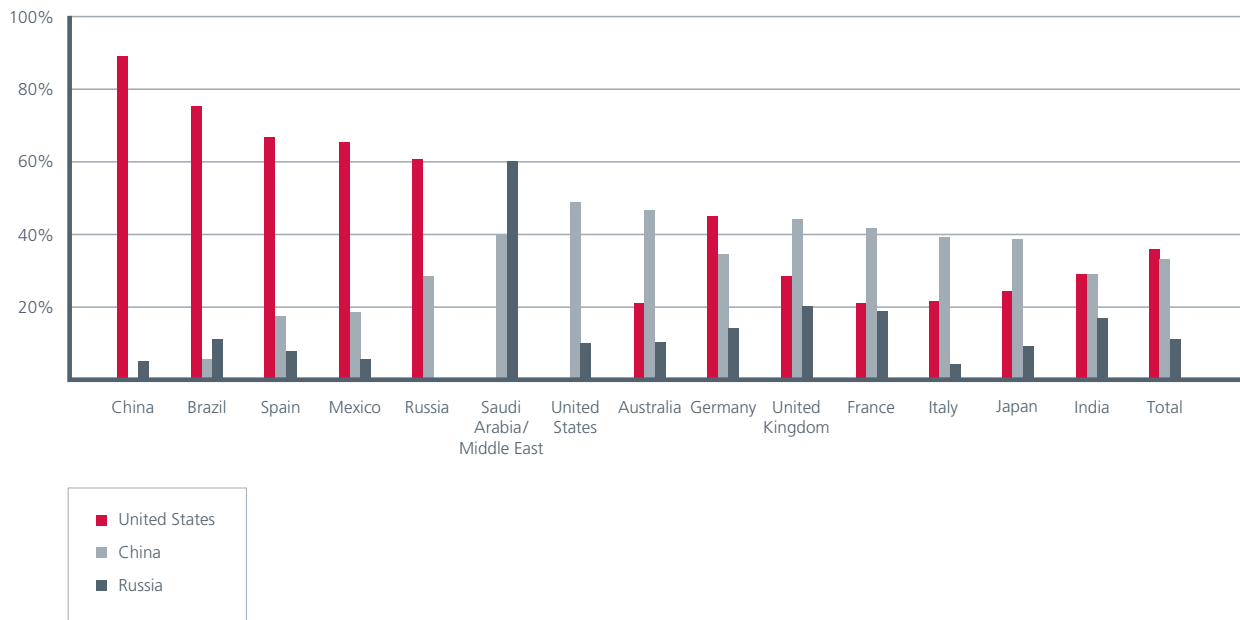
“The aggressors we face [in Australia] are economic aggressors... it very much depends on the sector,” said Ghosh, the Australian security executive. “The mining sector sees China as more of a threat... In the defense sector, the competitors are Europe and United States.”

The United States was seen as the most worrisome potential aggressor by large majorities of executives in countries where broader suspicions of U.S. motives are common—China (89 percent), Brazil (76 percent) Spain (67 percent) Mexico (65 percent) and Russia (61 percent). But even in a traditional U.S. ally like Germany, 45 percent named it the top concern, while only 34 percent named China, even though Germany’s government has publicly rebuked China for conducting computer network intelligence operations on key national assets.

“That [result] might be less shocking than it seems,” observed Hayden. “It might simply be a reflection of the raw capabilities and frankly the raw size of U.S. intelligence agencies.” The U.S. government has also engaged in a series of public, drawn out and largely unresolved policy debates about how to organize its network defense and attack capabilities. This ongoing public discussion may have created “an echo chamber” for concern about U.S. capabilities, said Hayden.

Although the U.S. debate attracted much more media attention, Russian officials have also engaged this year in a series of legislative measures aimed at giving authorities greater freedom of action against perceived attacks and threats. A newly proposed law would give Moscow authority to define and respond to acts of cyber war. The new law “essentially says that if they can determine that they have been targeted by a government of another state in a cyberattack, of whatever kind, they can treat it as an act of war,” Kimberly Zenz a Russia specialist at iDefense Labs, said.

Percentage naming the US, China or Russia as the country of 'most concern' in relation to foreign cyberattacks



Taken together, the new laws codify sweeping new powers for the Kremlin, she said. “If they do have a major incident, they can decide on their own who they think it was, and take action on their own at a very high level without needing any outside agreement or proof.”

China too has publicly disclosed information about its network warfare plans. A 2009 review of open source Chinese military literature by the U.S.-China Economic and Security Review Commission concluded that Chinese “campaign doctrine identifies the early establishment of information dominance over an enemy as one of the highest operational priorities in a conflict,” noting that a new strategy called “Integrated Network Electronic Warfare” appeared designed to fulfill this goal by integrating cyber and other electronic warfare techniques with kinetic operations.


Despite these discussions, there are clear limits to transparency. Both Russia and China, for instances, have faced—and flatly denied—well-documented accusations that they make common cause with nationalistic hackers. All three of these countries clearly intend to continue availing themselves to a greater or lesser extent of the strategic advantage that “plausible deniability” offers in cyberspace.

How can we move away from the “state of nature”?

As long as major governments desire unimpeded operational freedom in cyberspace, it will continue to be the Wild West. In the meantime, the owners and operators of the critical infrastructure which makes up this new battleground will continue to get caught in the cross-fire—and may indeed need what amounts to their own ballistic missile defense.

Improving Security in an Age of Cyber War





When it comes to strategies for improving cybersecurity, the data offers no easy answers.

When it comes to strategies for improving the cybersecurity of critical infrastructure, the survey and interview data offer no easy answers.

Critical infrastructure owners and operators reported that security is a top priority for them, and this is largely borne out by the wide range of security measures they deploy. But even sectors and countries with high rates of deployment of proven security measures are not free from attack.

“There is no identifiable protection model that will keep pace with the evolution and sophistication of cyber threats,” says the power sector’s Michael Assante. In addition, innovative technologies, from cloud computing to “Smart Grid” meters and SCADA connectivity, continue to create new vulnerabilities.

Governments are also searching for the best approach to cybersecurity for their infrastructure. Two challenges are common to their efforts:

- Modifying old government structures and organizations to deal with cyber threats to critical infrastructure; and
- Finding useful ways to share sensitive information about threats and vulnerabilities with owners and operators and to deploy sensitive capabilities to help critical infrastructure defend itself.



Some key security technologies remain underutilized

Authentication standards in particular need improvement, and the take up of biometric technology remains low. Network security increasingly depends on detecting and stopping users whose accounts show anomalous behavior or exceed a strictly defined set of privileges. And attackers are increasingly targeting users on an individual basis through phishing and other strategies. These developments mean that authentication of users and their privileges are growing in importance.

Yet over half of all executives (57 percent) said their organization employed only user-names and passwords to authenticate those logging in. The remainder used stronger authentication techniques, like biometrics or tokens, either singly or in combination. Overall, only 16 percent said they used biometrics—a low take-up rate some experts attribute to cultural resistance in many countries. Tokens were more than twice as popular. There are drawbacks, technical challenges and cost factors in the use of biometrics and tokens, said experts, and password/login combinations can vary greatly in effectiveness, depending on the strength of the passwords used and the encryption technology employed. But additional layers of security are clearly preferable to the simple use of usernames and passwords, which are often too easy to guess, steal or otherwise compromise.

Similarly, on a global basis, only about half of the executives reported using encryption routinely under most circumstances, although it was more common for online transmission of data, where 61 percent reported using it. This too seems low, especially as the use of mobile devices grows. Pamela Warren, a cybersecurity expert working for McAfee, believes that, “if you’ve got mobile devices and you have sensitive data on those devices, then you absolutely should be looking to encrypt that data.”

Vulnerabilities continue to expand

The increased use of IP networks for SCADA and other operational control systems creates unique and troubling vulnerabilities. Executives with SCADA/ICS responsibilities reported high levels of connections of those systems to IP networks including the Internet—even as they acknowledged that such connections create security issues. Sector experts expressed grave concern about the security implications of this development, and IT security specialists stressed the need to mitigate this threat.

Remote access to control systems “poses a huge danger,” said Dr. Phyllis Schneck, McAfee’s vice president of threat intelligence. “We must either protect it appropriately or move it to more private networks and not use the open Internet,” added Schneck, a member of CSIS’ Commission on Cybersecurity for the 44th Presidency.

Over half said their organization employed only user-names and passwords to authenticate those logging in.



“There is a level of protection afforded by virtualizing older software on top of newer software, so that at least the protocols and the network access travels through newer software stacks,” added one veteran IT security specialist. He said owners and operators “need to put as many hurdles as [they] can put against an attacker.”

“The goal [for quickly securing SCADA systems] should be not necessarily to hold [or] replace those systems, but to put blocking technologies, to the extent possible, in front of them and to have much more rigorous criteria for accepting new systems in the future.”

SCADA risk is compounded by emerging “smart” delivery platforms

New service delivery platforms like the interoperable “smart metering” of electricity or banking on mobile devices create new vulnerabilities, but also offer new opportunities. “The smart grid will absolutely create new vulnerabilities, but that doesn’t mean that the entire energy system will be more vulnerable in the future,” said former U.S. Department of Energy cybersecurity official Christopher “Rocky” Campione, adding there were pay-offs in the form of improved efficiency and reliability.

Whether the savings outweigh the risks remains to be seen. One challenge looming in the development of smart metering is keeping the cost low enough for mass-market adoption. The security implications of that pressure are troubling. “How much security can you build in if your unit cost needs to be less than a hundred dollars?” asked one expert.

In a quickly changing environment, IT and security executives find themselves having to make difficult calculations about security with limited information, said Campione. “You have to make decisions that weigh opportunity, risks and security, but you do not want to get trapped in ‘analysis paralysis.’ You can’t know everything before you decide.” In such an environment, it is not clear how much attention has been paid to the security tradeoffs that come with a “smart grid.”

Cloud computing too presents new security challenges

Cloud systems allow companies to lease server infrastructure and software services—effectively outsourcing their computing requirements. Depending on the services and data being outsourced, it can offer new security measures as well as creating new vulnerabilities.



Many governments continue to wrestle with the “org chart” question, and in some cases the result is a work in progress.

Cloud computing allows smaller enterprises to utilize security measures that would not otherwise be available to them. Even so, “cloud computing scares the hell out of me,” said the veteran IT security specialist. “Not because I know of any particular specific problem inherent to it, but because, historically speaking, every time we have moved into a new area we have failed to appreciate what new potential for attacks has been created.”

“We are creating yet more complex systems, and yet more systems that depend for their value on providing services to loosely coupled or loosely authenticated other systems,” he concluded.

Warren said to mitigate vulnerabilities businesses and governments should “consider the types of data that could be moved to the cloud and the best cloud model for the given business, vet the security model and practices of the service provider, and set guidelines for hosting accountability.”

Governments need to be better organized to confront cyber threats

One issue which cropped up repeatedly in interviews with experts from different sectors and countries was the way governments were organizing themselves to confront the new threat. There are common models—all of the countries surveyed, for instance, had established Computer Emergency



Response Teams (CERTs), to handle incident response, although their effectiveness varied, according to interviews. But many governments continue to wrestle with the “org chart” question, and in some countries the result is clearly a work in progress.

In Brazil, for example, the federal government in August 2009 established the Critical Infrastructure Protection Information Security Working Group, under its Department of Information and Communications Security. The group is working on information security and incident response plans, according to IDefense labs Brazilian analyst Anchises de Paula.

In Australia, a 2009 defense white paper announced the establishment of a national Cyber Security Operations Center, within the military's Defense Signals Directorate, but many details have yet to be announced.

One Australian cybersecurity specialist said his government spent a lot of time studying the U.S. and UK models, as well as others, as part of its recent cybersecurity policy review. “There is something of a standoff between elements of government that prefer the U.S. model and those that prefer the UK model,” he said.



Because critical infrastructure tends in many countries to be already regulated, these kinds of changes can create problems for owners and operators with conflicting or over-lapping regulatory or other government demands regarding cybersecurity. Executives are often more comfortable with their legacy regulators and concerned by or suspicious of new or changed regulatory demands. But those regulators often lack sophistication about cybersecurity matters.

U.S. water sector security specialists told us, for example, that they had a very good relationship with their traditional regulator, the Environmental Protection Agency, but they recognized it was unrealistic to expect it to regulate cybersecurity as well. "There is no way that EPA is going to have any kind of regulatory control over the country's cyber infrastructure," one said.

The existence or creation of multiple agencies with regulatory authorities, investigative powers or security responsibilities with regard to cybersecurity can also give rise to bureaucratic friction within governments.

For example, Kimberly Zenz said that turf conflicts on the issue of cybersecurity were rife in Moscow. "There's a lot of infighting in Russian government organs. There's fighting at every level. All the federal organisations, even within the same ministry, are all fighting each other."

In the United States, friction in the executive branch is duplicated and amplified by conflicts between oversight committees in Congress. "Capitol Hill has absolutely no understanding of cybersecurity issues in the United States," said former Department of Energy official Campione. "There is a molasses effect," he added, concluding that the root of the problem was the way the U.S. government was funded. "If, as a lawmaker, you [allocate funds] to the central CIO's office [of an agency], that money is going to end up in Washington, or at least end up being spent by people in Washington. If you give the money to some bureau [some sub-department of an agency] then it ends up in West Virginia... or Pittsburgh or wherever it is that you want it," said Campione.

"The drivers for spending on the Hill are highly geographical." This, he added, "is why all these government departments have a difficult time consolidating their IT."

Information-sharing seems to work better horizontally

Executives reported higher levels of participation in more horizontal, industry-to-industry information-sharing bodies, although different countries had different structures for these organizations and differing participation levels.



Information sharing between software security companies, for instance, “has made tremendous progress in overcoming challenges in trust, [intellectual property law] and competitive landscape,” said McAfee’s Phyllis Schneck. She said the sector “work[s] well together... especially in a time of crisis.”

An even greater variety of approaches characterized the organization of government to industry information-sharing forums, and there was wide national variation in participation rates reported. But here, in the interview data at least, a common complaint could be heard: governments are reluctant to share sensitive information about threats and vulnerabilities.

The chief security officer for a large telecommunications provider says his firm has relationships with law enforcement in more than a hundred countries where it operates. But when it comes to sharing security information about critical national infrastructure, none of them “have anything as comprehensive as I would want to see. What I want from any government is something I can’t produce myself—intelligence on what [the] threats are, where we could better utilize our assets on the basis of more detailed threat analysis than I can provide. They’ve got all their security services and other capabilities.”

But that is exactly the kind of information that governments tend to guard most jealously, in part because they see no sure way to share the information with critical infrastructure owners and operators that does not also disclose the information to adversaries.

For this reason, high levels of participation in government-led information sharing bodies might not be a good measure of their success. Some countries clearly adopt a more exclusive approach to information-sharing than others.

Secrecy and security

“In the United States and Europe there’s a little more effort” on the part of agencies to share information, said the CSO, “But when it comes to getting truly useful information back from the government—warnings or advice about the use of resources—[we get] nothing at all, from any government.” In the United States, where executives reported a higher than average membership in government information-sharing groups, attempts have been made to address these issues through granting clearances to critical industry executives, but progress has been uneven.

The data shows a uniquely close relationship between critical industries and government in China.

“One or two people [in a given firm] have a clearance,” said Campione, “and it might not be the right person.” Should the clearance be held by a senior executive who might not have the technical expertise to interpret what he or she was told? Or by a more technically adept but more junior staffer who might lack the authority to deal with problems he cannot disclose to others?

Another approach, advocated by McAfee’s Pamela Warren, is to declassify more information to a “sensitive but unclassified” level, information that is “sharable among members of a trusted community” including with those without clearances. “Definitely part of the problem is we’re classifying too much,” said the former energy official.

In Australia, security executive Ajoy Ghosh said that the new national Cyber Security Operations Center would have operational capacity, the ability to put “boots on the ground” alongside owners and operators of critical infrastructure. In the United States, by contrast, agencies have favored an approach based more on standards-setting.

In Russia, Zenz said, government favored a more informal approach. Although there is no national cyber exercise plan and little institutional provision for information sharing or partnership, government officials “have very close relationships with the ISPs... and within the ISPs there are people who have real-time network awareness” and keep them informed, she said.

A uniquely close relationship between industry and government in China can be found in the data showing high levels of participation in and approval of government-led security initiatives. Whether that relationship can be replicated elsewhere is open to question, however. Gen. Hayden noted that “it’s a more authoritarian state so it might be easier for them to do that... The population perhaps... is more accustomed to the demands of security... given all aspects of Chinese life and culture” and the fact that Internet usage there, though large and growing is still limited to “a very select fraction” of the population.

The difficulty of working effectively with industry is compounded by the fast-moving nature of the threat. One U.S. transportation sector security specialist told us, “The currency of operational expertise drops off quickly [once an industry executive joins] government. This is a major problem that the sector faces when dealing with their respective agencies.”

Indeed, the same problem haunts efforts to engage the public in a realistic security dialogue. Public debate on security issues always presents challenges but they are especially acute in the cyber domain, argued Gen. Hayden. “You get one or two steps out of the starting gate and you have left 95 percent of the audience behind technologically... then the privacy advocates come out the conversation suddenly becomes very difficult... It is very hard culturally for us to do this.”

Conclusion

The survey data shows that computer networks, especially IP-based ones, are now essential to critical infrastructure owners and operators. In the current economic climate, owners and operators, who use IT to improve efficiency, will increase their reliance on networks, in both operational and administrative systems. The data and the interviews show that those critical systems—including operational ones like SCADA/ICS—are operating in a high threat environment, and facing a range of risks, including some very expensive ones. But they also suggest that much can be done to protect those systems, for example through more widespread adoption of key security measures.

If cyberspace is the Wild West, the sheriff needs to get to Dodge City. Governance issues are front and center in any discussion of network security for critical infrastructure. There was a wide range of commentary for example about legal barriers to the possibility of the more widespread use of use technical measures to counter DDOS attacks. And experts discussed the difficulties facing treaties and other efforts in this area.

For owners and operators, the survey shows, their relationships to governments are a key factor in how they handle security. For governments, that relationship is crucial for the defense of national assets. In the absence of technological silver bullets, many executives see regulation—despite its drawbacks—as a way of improving security. And beyond just regulation, the data suggests that in some countries, most notably China, a close relationship between government and owners and operators has helped improve security.

Acknowledgements

CSIS researchers and authors spoke formally and informally to dozens of people while working through the huge amount of data gathered for this report. Many agreed to be formally interviewed and quoted, but not all were happy to be named, even here in the acknowledgments where they are safely separated from their words. We are grateful to everybody—named and unnamed—who gave so generously of their time and insight. Special thanks are owed to James Lewis for his advice and counsel and Denise Zheng, who kept the project on track. Naturally, the authors acknowledge themselves fully responsible for any errors or omissions.

Stewart Baker, distinguished visiting fellow, CSIS; partner, Steptoe & Johnson

Shaun Waterman, writer and researcher, CSIS

George Ivanov, researcher, CSIS

Michael Assante

vice president and chief security officer,
North American Electric Reliability Corporation

David Aucsmith

senior director, Microsoft Institute for
Advanced Technology in Governments

Christopher “Rocky” Campione

former senior cybersecurity official, U.S. Department of Energy

John Carlson

senior vice president, BITS,
a division of the Financial Services Roundtable.

Claudia Copeland

specialist in resources and environmental policy,
Congressional Research Service

Dan Corcoran

group information security officer, Consumer Group at Intuit

Kristen Dennison

threat intelligence analyst, iDefense Labs

Ajoy Ghosh

security executive at Logica and lecturer
in cybercrime at the University of Technology, Sydney

Gen. Michael Hayden (retired)

former director, Central Intelligence Agency;
former principal deputy director of national intelligence;
former director, National Security Agency

Rick Howard

director of security intelligence, iDefense Labs

Aaron Levy

manager of security policy,
Association of Metropolitan Water Agencies

Anchises De Paula

threat intelligence analyst, iDefense Labs, Brazil

Karl Rauscher

distinguished fellow
EastWest Institute; fellow, Bell Labs

Adam Rice

global chief security officer, Tata Communications

Phyllis Schneck

vice president of threat intelligence, McAfee; member, CSIS
Commission on Cybersecurity for the 44th Presidency

Paul Smocer

vice president, BITS, a division of Financial Services Roundtable

Pamela Warren

cybercrime strategist, public sector and
telecom initiatives director, McAfee

Tom Wills

Financial Services ISAC and iDefense Labs

Kimberly Zenz

threat intelligence analyst, iDefense Labs.

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 2005–09, 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 1992–94, he was general counsel of the National Security Agency.

Shaun Waterman is a journalist and consultant on terrorism and national and homeland security issues, contracted by CSIS to research and write this report. Currently a freelance reporter for the Washington Times and other publications, he was from 2000–09 a senior correspondent and editor at United Press International in Washington.

George Ivanov is a CSIS researcher and a master's degree candidate in International Science and Technology Policy at George Washington University.

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

About McAfee

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, 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.

For more information, visit:
www.mcafee.com



McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any other non-McAfee related products, registered and/or unregistered trademarks contained herein is only by reference and are the sole property of their respective owners.

The information in this document is provided only for educational purposes and for the convenience of McAfee's customers. We endeavor to ensure that the information contained in the McAfee Virtual Criminology Report is correct; however, due to the ever changing state in cybersecurity the information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

© 2009 McAfee, Inc. All rights reserved.

7795rpt_cip_0110