2011 Symantec Critical Infrastructure Protection Survey

GLOBAL FINDINGS

Symantec

CONTENTS

Executive Summary

To understand the concept of critical infrastructure, imagine a day without it. You wake up with no power. All phones are down. Gas is unavailable, and forget the bus, train or subway because they are inoperable as well. Even going to the store for food isn't an option. Not that it would matter because the banking and finance system has been disabled as well.

You get the picture. Even disruption of *one* of these 'critical infrastructures' would wreak havoc on our world. Because of the implications of a critical infrastructure threat, governments around the world have established critical infrastructure programs. The goal of government Critical Infrastructure Protection (CIP) programs is to protect against network-wide attacks that aim to shut down one or more critical infrastructures.

Today, CIP providers worry about attacks specifically focused on their networks. For example, in 2009 cyber spies penetrated the U.S. electrical grid leaving malware that could have been used to disrupt U.S. power systems.

Now in its second year, the **2011 Symantec Critical Infrastructure Protection Survey** explores government CIP programs in general and three areas specifically:

- The engagement level of critical infrastructure providers with their government's CIP programs.
- The threat level based on reports from critical infrastructure providers.
- The readiness level of critical infrastructure providers.

Last year we found a high level of engagement, threat and readiness among critical infrastructure providers. In 2011, results showed a reduction in all of these areas. This year's survey introduces three new indices that combine a broad array of measurements to better understand the state of today's government CIP programs:

- The **CIP Participation Index**, a composite of a broad array of measures, shows how positive industry's attitudes are about government CIP programs, as well as how engaged they are.
- The **Threat Index** measures attacks in the past 12 months, their effectiveness, and how critical infrastructure providers believe the threat will change over the next 12 months.
- The **Readiness Index** shows the readiness of organizations overall as well as in a variety of specific areas.

The results of these indices told us critical infrastructure providers are *less engaged* with their government's CIP programs, *less concerned* about the threats and *less ready* than 12 months ago.

Methodology

Applied Research fielded the survey by telephone during August and September of 2011. They surveyed the following 14 critical infrastructure industries (8 more than last year):

1. Finance and insurance
2. Telecommunications
3. Public services (law enforcement, fire and emergency, other)
4. Energy
5. Medical, health care and welfare
6. Information technology
7. Agriculture and food processing
8. Aviation – aircraft, air traffic control, airports
9. Government
10. Manufacturing
11. Mass transit & rail
12. Pharmaceuticals
13. Public works (water and waste water)
14. Chemical products

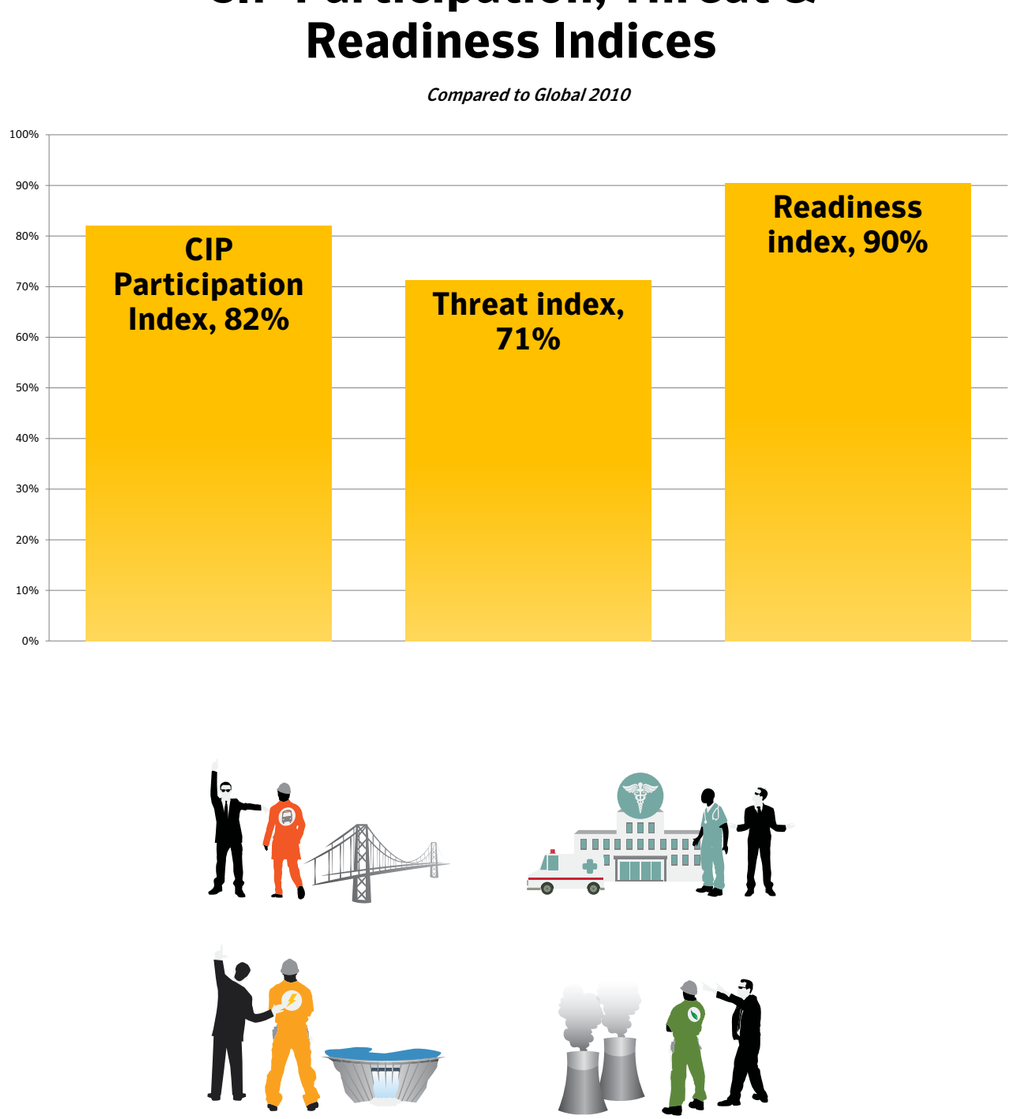
Applied surveyed 3,475 organizations in 37 countries, split between small businesses (5 to 499 employees) and Enterprises (> 1,000 employees in the US, > 500 employees outside the US).

Note: For less developed countries, Applied used the number of PCs as a measure of company size rather than employees. This controls for countries that have large numbers of unskilled laborers.

For SMBs, Applied spoke with the 'person in charge of computers.' For Enterprises, Applied spoke with a mix of C-level and senior IT management.

The confidence level for this survey is 95 percent accuracy with a +/- 1.7 percent margin of error.

NOLA is comprised of Colombia, Costa Rica, Panama, Dominican Republic, Puerto Rico, Peru, and Guatemala and SOLA is comprised of Argentina, Chile, Uruguay, Paraguay, and Bolivia.



CIP Participation, Threat & Readiness Indices

Compared to Global 2010

Finding 1

Lower Awareness and Engagement in Government CIP Programs

What a difference a year makes. In last year's survey we found surprisingly high awareness and engagement in government CIP programs. This year that awareness and engagement has dropped somewhat as measured by the CIP Participation Index.

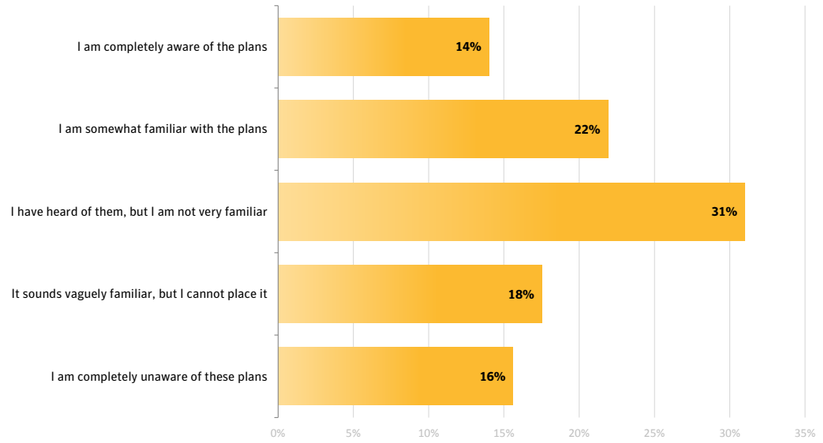
What caused the drop in the CIP Participation Index? Several things: First, companies were generally less aware this year of their government's CIP programs (36 percent were somewhat or completely aware this year compared to 55 percent last year). Second, companies proved to be less engaged in CIP programs as compared to last year (37 percent this year versus 56 percent last year).

The survey also indicated that government CIP programs are relatively new to many companies, with only 17 percent responding that their company has been engaged with their country's critical infrastructure plans for 1 to 2 years and 12 percent responding their engagement has lasted more than 2 years.

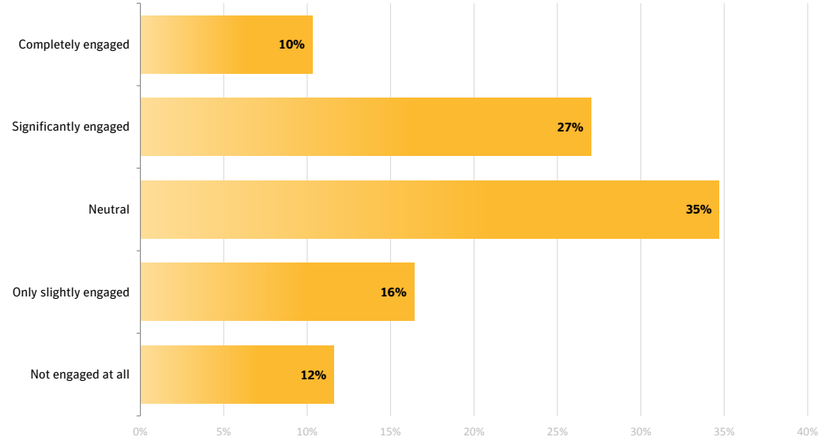
"I'm aware of the programs, but I don't like them. They have enough on their plate so it needs to be company motivated."

IT manager for an energy distribution company

What is your awareness of the critical infrastructure plans being discussed within your country?



How engaged is your company with the critical infrastructure plans being discussed within your country?



CIP Participation

Has your country included your sector in their CIP plans?
50% yes
20% no

Overall opinion of CIP plans taking place in your country?
44% positive
14% negative

Willingness to cooperate with your country's CIP plans?
57% willing
10% unwilling

Length of involvement with your country's CIP plan?
71% 0-1 year
29% 1+ year

Finding 2

Slightly More Ambivalence About Government CIP Programs

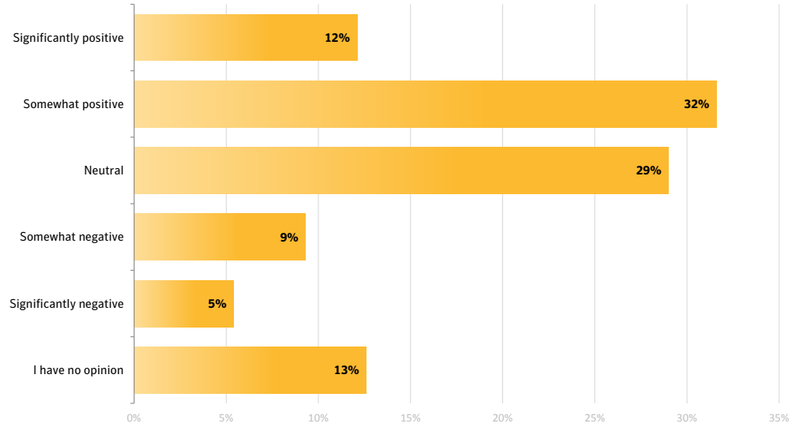
Furthermore, we uncovered evidence that companies are more ambivalent in 2011 than they were in 2010 about government CIP programs. For example, when asked to voice their opinion about government CIP programs, more chose 'neutral' or 'no opinion'. Plus, they are now slightly less willing to cooperate with government CIP programs than they were one year ago (57 percent versus 66 percent).

Despite the survey results indicating an uptick in ambivalence, when respondents were asked to choose words that reflected their reaction to the critical infrastructure plans being discussed in their country, positive words like accepting (30 percent), appreciative (22 percent), and enthusiastic (18 percent) ranked higher than negative words such as skeptical (14 percent), wary (11 percent), and resistant (6 percent).

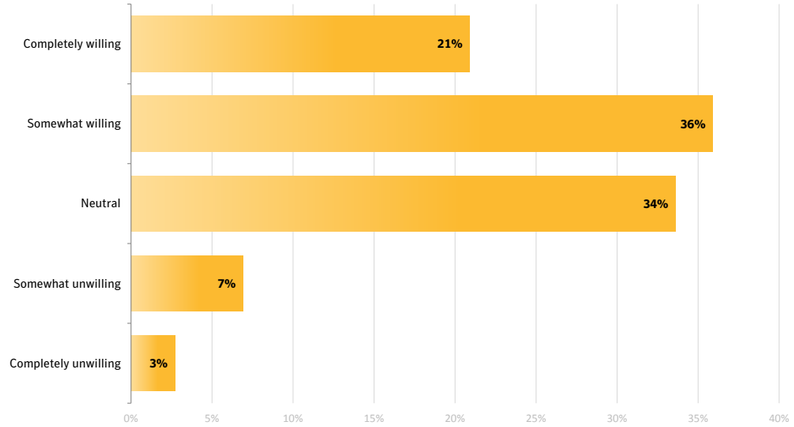
"We constantly run audits on our equipment to find vulnerabilities, I think that should suffice."

IT manager from a mass transit company

What is your overall opinion of the critical infrastructure plans being discussed within your country?



How willing are you to cooperate with the critical infrastructure plans being discussed within your country?



Finding 3

Organizations feel less prepared

It is not surprising that as an organization's assessment of the threat drops, their readiness drops as well. For example, overall readiness fell an average of 8 points in 2011 (60 to 63 percent this year versus 68 to 70 percent of companies reporting they were 'somewhat' to 'extremely' prepared last year).

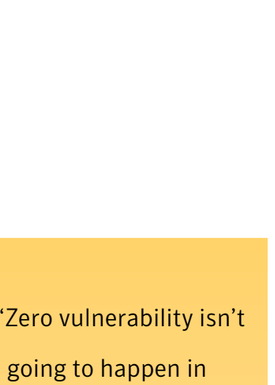
In terms of the following specific safeguards, the survey noted a decrease of 5 to 10 percent in readiness:

- Network security measures
- Messaging security
- Website security
- Endpoint security
- Security monitoring
- Access control to infrastructure and information based on user credentials
- Disaster recovery planning
- Security audit
- Security response
- Security training
- Awareness and appreciation of threat by executive management.

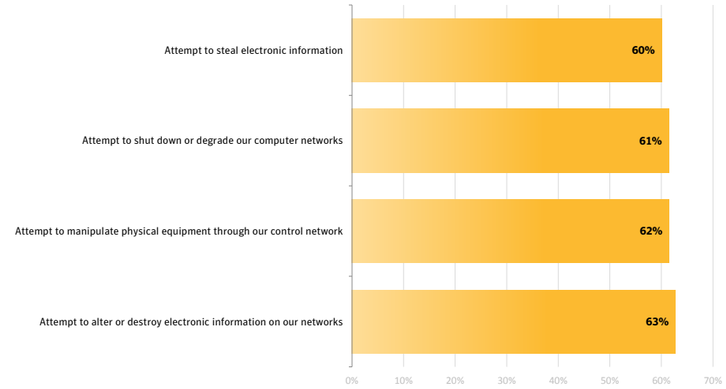
So, what does Symantec recommend for companies who are involved in critical infrastructure industries?

"Zero vulnerability isn't going to happen in the real world. We are probably about 30% vulnerable."

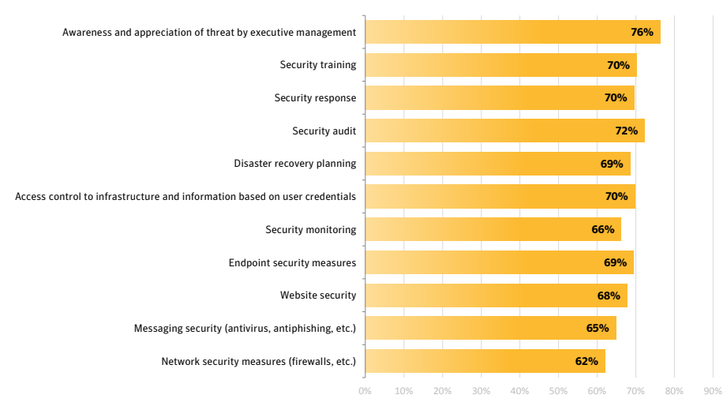
IT manager for a food processing company



Overall, what is your readiness to withstand the types of attacks we have been discussing? (Somewhat/Extremely prepared)



Overall, what is your readiness to withstand the types of attacks we have been discussing? (Not a high state of readiness)



CIP Readiness

Engagement in your country's CIP plans?

37% engaged

28% slightly/not engaged

Readiness to withstand attacks?

60-63% somewhat/ extremely prepared

11-14% somewhat/ extremely unprepared

Key Recommendations

To ensure resiliency against critical infrastructure cyberattacks, follow these steps:

- **Develop and enforce IT policies and automate compliance processes.** By prioritizing risks and defining policies that span across all locations, organizations can enforce policies through built-in automation and workflow and not only identify threats but remediate incidents as they occur or anticipate them before they happen.
- **Protect information proactively by taking an information-centric approach to protect both information and interactions.** Taking a content-aware approach to protecting information is key in knowing who owns the information, where sensitive information resides, who has access, and how it is coming in or leaving your organization.
- **Manage systems** by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.
- **Protect the infrastructure by securing endpoints, messaging and Web environments.** In addition, defending critical internal servers and implementing the ability to back up and recover data should be priorities. Organizations also need the visibility and security intelligence to respond to threats rapidly.
- **Ensure 24x7 availability.** Organizations should implement testing methods that are non-disruptive and they can reduce complexity by automating failover. Virtual environments should be treated the same as a physical environment, showing the need for organizations to adopt more cross-platform and cross-environment tools, or standardize on fewer platforms.
- **Develop an information management strategy that includes an information retention plan and policies.** Organizations need to stop using backup for archiving and legal holds, implement deduplication everywhere to free resources, use a full-featured archive system and deploy data loss prevention technologies.

For government to promote critical infrastructure protection, Symantec recommends the following:

- **Continue to put forth the resources to establish critical infrastructure programs.** The majority of critical infrastructure providers confirm that they are aware of government critical infrastructure programs. Furthermore, a majority of critical infrastructure providers support efforts by the government to develop protection programs.
- **Partner with industry associations and private enterprise groups to disseminate information to raise awareness of CIP organizations and plans**, with specifics about how a response would work in the face of a national cyberattack, what the roles of government would be, who the specific contacts are for various industries at a regional and national level, and how government and private business would share information in the event of an emergency.
- **Emphasize that security is not enough to stay resilient in the face of today's cyber-attacks**. Government should also emphasize to critical infrastructure providers and enterprises that their information be stored, backed up, organized, prioritized and that proper identity and access control processes are in place.