Protecting Critical Infrastructure

In today's global arena, many companies are vital components of a nation's "critical infrastructure." Countries and companies must collaborate now, more than ever, to protect the services essential to a nation. Threats to a company's information systems and assets could come from anywhere. "Whether the incident comes as a direct physical attack or an electronic one," says John N. Stewart, VP and CSO of Cisco, "the nature of these events is essentially borderless." No single company could possibly possess all of the intelligence, expertise and resources needed to combat threats originating from such a plethora of fronts. So where does a company turn for help to acquire the necessary information, develop policies and strategies, and coordinate operational responses to an attack?

:: Seeking out complementary core competencies

In response to escalating worldwide threats, companies in the United States and across the globe have begun developing close partnerships with their government counterparts to enhance infrastructure security. These public-private partnerships enable both parties to exchange vital information, resources and expertise, create risk management plans and conduct response drills to ensure readiness against potential threats.

"Government agencies possess unique core competencies that complement private-sector strengths," explains Ken Watson, manager of the Critical Infrastructure Assurance Group for Cisco. "Intelligence services and first responders — including emergency medical technicians, firefighters and law enforcement officials — are the unique responsibility of governments." Furthermore, governments have a broad cross-sector perspective, enabling them to consider interdependencies across multiple industries and public entities that would not normally be part of a single company's risk planning. These might include everything from power and water to transportation and financial services.

Why public-private partnerships are essential to your company's security

CSO Custom Solutions Group

cisco

In the United States and elsewhere, where much of a nation's critical infrastructure might be in the hands of the private sector, working collaboratively provides companies and government entities a practical solution for understanding and protecting the interdependencies that are not only vital to a nation's security but also to the health and well-being of its citizens.

:: Tips on managing public-private partnerships

While Stewart acknowledges that public-private relationships are complex, he reasons, "You have to invest the time and energy in building trust before things go askew, so that when you have to work through a crisis or a disaster, you already have relationships that are strong and responsive." So how does one nurture public-private partnerships while protecting trade secrets and vulnerabilities from competitors and destructive outside forces?

Meet your public-sector counterparts face to face. It's easier to build trust sitting down over a cup of coffee than anonymously through e-mails.

Attend government forums and briefings. The U.S. Secret Service and Federal Bureau of Investigation, Interpol in the United Kingdom, India's Special Services Unit and other law enforcement organizations around the globe offer forums for companies of every size and sector. Also, organizations focused on intelligence or special missions, like the U.S. Department of Homeland Security, hold forums and meetings in their areas of specialty. This is a way to reach out and learn not only what government agencies can do but what capabilities reside in companies within your sector.

- **Get involved in legislative reform.** If your company is going to be subject to local, provincial, state or federal laws that affect your company or sector, it's important to understand how those regulations and legislation are evolving. You want to educate lawmakers to the best of your ability, so that any new provisions they create don't result in unintended consequences for you or your industry.

- **Maintain information security contacts in all the countries in which you operate.** Assign someone in each of your facilities to develop a trusted list of first responders they would contact in an emergency. And make sure they keep the lists current. Once an incident occurs, it's too late to make random phone calls to generic numbers and try to build trusted relationships on the fly. When you're in the middle of a crisis, you don't have the luxury of time to educate an anonymous responder on your company and what support it needs.

- **Participate in your industry ISAC (Information Sharing and Analysis Center)** or its equivalent *(see www.isaccouncil.org).* These centers represent a trusted community of security specialists from companies across a single industry sector dedicated to protecting their infrastructures by identifying and sharing best practices to quickly and properly address vulnerabilities. As appropriate, they share information and interact with government agencies that can enhance their and other sectors' readiness in a threat.

- **Join FIRST (Forum for Incident Response and Security Team, *www.first.org*).** This organization provides trusted peer relationships with incident response teams from other companies and governments. FIRST allows you to share incidents one-on-

While the number of sectors that have ISACs continues to expand to address growing threats to physical and cyber security, currently the list includes councils for critical infrastructure in:

:: Communications (www.ncs.gov/ncc/main.html)
:: Electricity (www.esisac.com)
:: Emergency management response (www.usfa.dhs.gov/emr-isac)
:: Financial services (www.fsisac.com)
:: Highway (www.highwayisac.com)
:: Information technology (www.it-isac.org)
:: Multi-state (www.msisac.org)
:: Public transit (www.surfacetransportationisac.org/SPTA.asp)
:: Surface transportation (www.surfacetransportationisac.org)
:: Supply chain (www.secure.sc-investigation.net/SC-ISAC)
:: Water (www.waterisac.org).

Membership provides you with a community of trusted colleagues—legally bound to protect the information you exchange—who can help you in a crisis.

"Public-private partnerships aren't about improving profits for a company. They're about defending corporate and government networks."

Ken Watson, Manager, Critical Infrastructure Assurance Group, Cisco

one with other teams while protecting sensitive information about those incidents. There have been numerous times where one company's incident response team traced the origin of an incident affecting its networks to another company's region and successfully coordinated its investigation and resolution. FIRST also provides smaller companies that have fewer security resources broader access to information on hot security topics. And like an ISAC, membership provides you with a wider community of trusted colleagues who can help you in a crisis.

:: Barriers to information sharing

As any corporate lawyer will tell you, be careful whom you trust. While it might be beneficial to share certain security information with the government, it is wise to have a protection policy in place that guards the sensitivity of the information you exchange. In the United States, for instance, the government can deem information classified. But the Freedom of Information Act can potentially undermine the best intentions of government agencies to protect your vulnerabilities from public release, which may include distribution to those that can harm your information systems or assets.

John Stewart of Cisco offers some suggestions:

- **Before you exchange any information, understand the context in which it will be made public.** For example, an incident-based matter within your company might be held to the highest level of privacy by law enforcement. But if the information involves a publicly regulated facility, it might automatically fall under public disclosure laws.

- **Interact with government officials in relation to the area of the government where they work and the outcome you expect.** For instance, you might share a generic solution to a security problem, knowing that the information will be made public. But if you share an incident that occurred in your company to gain insight on how government can use that kind of information in the future, be prepared to answer questions regarding your disclosure. Work with your company's legal counsel to determine the correct course of action.

- **Remaining silent carries its own risks.** While individual companies have tended to keep their concerns to themselves, those looking to exploit critical vulnerabilities are collaborating aggressively on the best ways to use technology against us. To level the playing field, industry and government must learn to work together to protect not only themselves but each other, which may involve trusting one another.

:: The value of public-private partnerships

If your company provides goods and services to the private sector, you can gain unique insight into how your customers actually use your products in a crisis and then redesign them accordingly. But in general, "public-private partnerships aren't about improving profits for a company," Ken Watson points out. "They're about defending corporate networks and nations, states or other legal jurisdictions. The value for companies in public-private partnerships is that they gain the additional knowledge they need to protect themselves that they wouldn't otherwise have, and they gain an appreciation of their government partner's concerns about how to protect itself." Watson identifies three levels of public-private partnerships, each with its own intangible benefits: policy and strategy, operational, and technical.

At the policy and strategy level, he points to the PCIS (Partnership for Critical Infrastructure Security) one of the first cross-sector coordinating councils created at the request of a federal agency that brought together owners and operators of critical infrastructure to address such fundamental issues as:

- How to share information among sectors
- Whether the products and services available were sufficiently secure to protect critical infrastructure
- Whether enough money was being spent on research and development of security tools
- How interdependencies among sectors affect responses to emergencies
- Whether government has the right call lists and points of contact across infrastructures to provide a coordinated response to physical or cyber threats

As a result of its initial meetings, PCIS divided into working groups to address issues in research and development, information sharing, public policy and

internal governance. Originally a U.S. initiative, the concept is quickly going global, with interest and some collaboration among organizations around the world.

At the operational level are the ISACs. These information-sharing and analysis centers provide valuable frameworks for interaction among industry sectors and the government to advance the physical and cyber security of critical infrastructure. The ISACs constantly gather reliable and timely information from members, commercial security firms, government agencies, law enforcement and other trusted sources, and disseminate reports and notifications on electronic incidents, threats, attacks, vulnerabilities, solutions, countermeasures, security best practices and other protective measures. ISACs provide mechanisms for systematic and protected exchange and coordination of this information, as well as thought leadership to policymakers on critical infrastructure security and information-sharing issues.

At the technical level, there are various organizations like the Network Reliability and Interoperability Council (NRIC), which develops standards and best practices in the telecommunications industry.

Cisco's Stewart says that ultimately, public-private partnerships are all about anticipating crises and preparing for them. "Public-private partnerships will cost you less than if you make it up on the fly and, in fact, may save you in the end from doing irreparable harm." ::

The value of readiness drills with public partners

The lessons learned from Cyber Storm

In February 2006, the U.S. Department of Homeland Security staged a government-led cyber-security exercise, called Cyber Storm, to test the defenses of government agencies and leading private-sector organizations. More than 115 organizations in the United States, Canada, Britain, Australia and New Zealand participated in this groundbreaking exercise to test a national response system that could be implemented across all industry and government sectors. The exercise not only dealt with mock attacks by hackers, but also simulated how to deal with bloggers who were intentionally spreading misleading information about the attacks. Experts depicted hackers who shut down electricity in 10 states, failures in vital systems for online banking and retail sales, infected discs mistakenly distributed by commercial software companies, and critical flaws discovered in core Internet technology. While it remains to be seen to what extent the exercise will help to mitigate the potential harm from future cyber attacks, Scott Algeier, executive director of the IT-ISAC, says that the simulation was invaluable in helping his organization learn what it needed to do to improve its response to a real attack.

According to Algeier, foremost was the need to increase the collaborative analysis capability within IT-ISAC membership. During Cyber Storm, the organization's contracted operations center was quickly overwhelmed with incoming information and requests for critical updates from participants. "It was often very difficult for the center's staff to separate the urgent from the important," explains Algeier. "As a result, IT-ISAC has decided that we will be getting our members engaged earlier in the response process to provide technical expertise and analysis."

IT-ISAC leaders emerged from the exercise with a few other important lessons. In working with the federal agency responsible for the government's cyber networks, they learned that it was crucial to work jointly on each other's concept-of-operations documents. In this way, they were able to familiarize themselves with each other's processes and ensure more streamlined information sharing. IT-ISAC also agreed to develop a 24x7 contact list within its member companies for the Department of Homeland Security to tap in case of an emergency.

But perhaps one of the most interesting findings from Cyber Storm was the reluctance of law enforcement and intelligence communities to approach experts in the private sector for help in analyzing sensitive or classified information, despite the fact that these individuals held the necessary security clearances. According to Algeier, the cyber-security exercise revealed two problematic areas. "First, the government needs to be better informed about the analytical skills and security credentials held by ISAC members. And second, we need to continue to push to change the culture from one of holding information to one of needing to share."