

CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Public-Private Partnerships: Essential for National Cyber Security

Key Message: Government agencies and private industry must build effective partnerships to secure national critical infrastructures.

Executive Summary

“While governments have a responsibility to their citizens to mitigate and control national security risks, they usually do not have the authority to directly control privately owned critical infrastructure and assets. In the United States, for instance, the majority of critical infrastructure – over eighty percent by some estimates – is owned by private firms.”

“Developing partnerships between government authorities and infrastructure owners and operators is a method to help ensure the stability and availability of critical information and communication technologies. Partnership between government and industry helps the government disseminate vital information about security threats and vulnerabilities, coordinate effective incident management, and understand the resilience of critical infrastructure. The same partnership can help industry become aware of information about threats and vulnerabilities to which it would not normally have access and improve industry’s ability to manage risk.” [1]

In this podcast, Sam Merrell and John Haller, members of CERT’s Resilience Enterprise Management team, and Philip Huff, Manager of Security and Compliance with the Arkansas Electric Cooperative Corporation, discuss the actions necessary to create public-private partnerships between government and industry to strengthen national cyber security efforts.

This podcast is the second in a series on best practices for national cyber security. The first podcast discusses [establishing national computer security incident response teams](#).

PART 1: COMMUNICATION, TRUST, AND INFORMATION SHARING

Definition of Public-Private Partnership

For most nations, the government (public sector) is responsible for protecting national critical infrastructures. However, elements of these are often owned and operated by a private sector (industry) organization.

Public-private partnerships are a means to an end – protecting critical infrastructures at the national level. Such partnerships serve as a mechanism to share information and share and mitigate risk.

Governments have essential information, and critical infrastructure owners and operators have hands-on access to information systems. Both roles are essential for managing national cyber security.

Strategic Goals for Partnerships

According to the CERT report *Best Practices for National Cyber Security: Public Private Partnership* [1], there are two top-level strategic goals:

- Facilitate communication between public and private entities
- Support the national cyber security strategy

Practices for Facilitating Communication

By way of example, after September 11, 2001, the U.S. government encouraged greater communication about critical system vulnerabilities between the government and critical infrastructure providers. The U. S. [Freedom of Information Act](#) was a barrier for private sector organizations. The law was changed to expand the definition of national security so that information shared by providers would not be subject to the law and therefore would not be disclosed.

Building strong trust relationships at the personal level is essential.

Another key practice is to clearly define communication methods, channels, and rules to determine, for example, who is going to store the information and how the information will be used.

This practice requires that information be appropriately classified and categorized so that methods, channels, and rules address the sensitivity of the information.

PART 2: PRIVATE SECTOR BENEFITS AND PAIN POINTS; PARTNERSHIP MODELS

Benefits for Private Sector Organizations

Benefits include

- being involved in crafting solutions and mitigations for dealing with new threats that make sense and are effective
- being able to provide input, and be heard and responded to
- as a result, being able to better determine how to mitigate threats and vulnerabilities
- buying into the solution

Industry risk models are typically based on historical data and threat probabilities. This approach is not always effective for dealing with new, emerging threats. Having access to real-time government threat information is helpful.

Pain Points for Private Sector Organizations

If a private sector organization does not have a trust relationship with their government agency partners, it is difficult to obtain relevant threat information. Receiving broad brush information or a threat description where there is no feasible solution destroys the dialogue.

Having people who play a role in both the government agency and the private sector organization can help bridge the gap.

There is a natural tension between sharing too much information and not sharing enough to be helpful and useful.

Models for Structuring a Public-Private Partnership

The report [1] describes 3 models as follows:

Hierarchy: An example is the [U.S. Department of Homeland Security](#) and its 18 critical infrastructure sectors. DHS schedules meetings and designs meeting forums.

- Pro: Usually have good rules for sharing information
- Con: May exclude some parties and thus may miss capturing some information

Community: An example is the North American Electric Reliability Corporation ([NERC](#)). Different groups with shared interests come together to share information, with each other and with the government. Another example is the U.K. Warning, Analysis (Advice), and Reporting Point ([WARP](#)).

- Pro: The group defines its own rules for exchanging information. A community model fosters broad outreach

and awareness.

- Con: May not be the best model for sharing sensitive information due to being more inclusive than exclusive

Third party facilitated: A separate legal entity sits between private industry and the government. This allows each party to share information that they may not be willing to share directly with an objective intermediary. The [SEI's CERT](#) Program is an example.

- Pro: Extra layer of information protection as well as offering a neutral venue; data can be shared and then anonymized. Depending on funding, the third party can add value that government and industry may not be able to on their own.
-

PART 3: NERC – A SUCCESSFUL PRIVATE-PUBLIC PARTNERSHIP

Background

The [North American Electric Reliability Corporation](#) (NERC) has been in existence since the late 1960s, as an industry standard-setting organization. It has recently received statutory responsibility to provide mandatory and enforceable standards across industry.

NERC's mission is to work with government and industry to ensure reliable electric power throughout North America.

NERC membership is mandatory for those engaged in providing electric power (there are over 1,900 organizations). That said, participation in the open dialogue that NERC fosters is voluntary. NERC conducts assessments and interacts regularly with those involved in critical infrastructure protection.

NERC reports to the Federal Energy Regulatory Commission ([FERC](#)) and also works closely with the U.S. Department of Homeland Security.

NERC Services

NERC operates the (Electric Sector) Information Sharing and Analysis Center ([ES-ISAC](#)), which is another venue that private sector organizations can use to share information.

NERC conducts compliance assessments and works collaboratively with industry on standards and threat mitigation.

By virtue of having people from both government agencies and private sector organizations, NERC is able to take government information, understand it, and translate it into strategies for industry participation.

NERC can notify all of its constituents of a current or emerging threat very quickly, via alerts.

Resources

[1] Haller, John & Merrell, Sam. *Best Practices for National Cyber Security: Public Private Partnership* (CMU/SEI-2010-SR-010). Software Engineering Institute, Carnegie Mellon University. [to be published by 2010 calendar year end]

North American Electric Reliability Corporation ([NERC](#))

U.S. Information Sharing and Analysis Centers ([ISACs](#))

U.S. Department of Homeland Security National Cyber Security and Communications Integration Center ([NCCIC](#))

CERT [website](#)

