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

Managing Risk to Critical Infrastructures at the National Level

Key Message: Protecting critical infrastructures and the information they use are essential for preserving our way of life.

Executive Summary

Critical infrastructures provide the services that allow our nations, economies, cities, and homes to function. They include energy, water, telecommunications, financial services, transportation – and the Internet, to name a few. These infrastructures are inter-dependent and the information that they process, transmit, and store serve as the lifeblood for their proper function and operation. Critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP) are high priorities on the agenda for all country governments.

In this podcast, Bradford Willke, the leader of CERT's information security assessment and evaluation efforts, discusses efforts toward establishing a national risk management program for critical information infrastructures.

PART 1: CRITICAL INRASTRUCTURES AND THEIR RELIANCE ON CRITICAL INFORMATION INFRASTRUCTURES

Key Critical Infrastructures

Critical infrastructures are those that provide services that we all depend on every day. They include:

- water
- electricity
- telecommunications
- transportation
- manufacturing
- and, of course, the Internet

Who Is Involved

Those that have roles and responsibilities in ensuring critical infrastructures operate as expected include:

- government agencies (policies, standards, regulations, governance)
- public and private sector owners and operators
- standards communities
- citizens as consumers of services

According to the U.S. National Infrastructure Protection Plan, 80-85% of critical infrastructures are owned and operated by private sector organizations.

Differentiating Critical Infrastructures and Critical *Information* Infrastructures

Energy, as an example of a critical infrastructure (CI), involves generation, transmission, and distribution of power. Reliable energy delivery supports national security, economic stability, and public confidence.

Critical information infrastructures (CII) or IT infrastructures provide the foundation of information systems and information that allow CIs to operate effectively. Often CIIs will span critical infrastructures. One example is telecommunications.

The IT sector is essential for purchasing and building software, providing web services, and ensuring Internet availability.

Understanding the interdependencies among infrastructures is key when addressing CI and CII protection (CIP, CIIP) at a computer system and network level.

PART 2: NATIONAL RISK MANAGEMENT FRAMEWORKS AND PUBLIC/PRIVATE PARTNERSHIPS

Risk Management Practices for CIP and CIIP; National Frameworks

Several organizations have created useful frameworks for managing the risks to CIP and CIIP at the national level. These include the International Telecommunications Union (ITU) and the Organization for Economic Cooperation (OECD).

Some of the initial risk management practices that are common to both of these frameworks are to:

- identify and assign sponsors
- identify and assign lead organizations
- assign resources for participating public and private sector organizations
- develop a national strategy
- make sure the legal foundations are present, including criminal and civil actions, both within a country and across borders
- develop incident response capabilities at the national level, sometimes referred to as CSIRTs (Computer Security Incident Response Teams) (Refer to The Real Secrets of Incident Management podcast for more information about CSIRTs.)
- create public/private, industry/government partnerships to ensure effective interaction between owners and operators, and to promote strong policy and regulation.

Other supporting practices include:

- developing information sharing mechanisms
- defining and selecting processes for risk assessment
- estimating impact of various types of events and defining potential consequences
- assessing vulnerabilities and threats
- identifying and examining critical assets

These practices are directed towards building a culture of security that aids in stabilizing economies, public welfare, and public safety.

ISO Standards

Standards such as ISO/IEC 27001 facilitate the improvement of internal effectiveness and performance at the organizational level, by recommending a Plan-Do-Check-Act cycle.

That said, such standards are not sufficient for governments seeking to protect their communities and for addressing organizational and critical infrastructure interdependencies. An example would be the energy sector's reliance on telecommunications, Internet, and IT.

Where Progress Is Being Made

Organizations tackling risks to CI and CII at national and global levels include:

- OECD
- Organization of American States
- ITU's Directorate for Development (ITU-D)
- APEC TEL

The U.S. government has helped stimulate the creation of Information Sharing and Analysis Centers (ISACs) for critical infrastructures such as energy and IT.

An ISAC is a vehicle to bring private and public sector organizations together for a specific CI sector. Part of an ISAC's mission is to address intra- and inter-sector dependencies.

PART 3: FIRST STEPS AND ADDITIONAL RESOURCES

Risk Management for Critical Infrastructures: Getting Started

Take an accounting of sector strengths and weaknesses including national and industry capabilities.

Examples of what to look for include:

- Is there a legislative footprint that addresses e-crime, electronic signature laws, identity management, etc? These are necessary controls and countermeasures for dealing with cybersecurity at a national level.
- What indicators are in place that reveal infrastructure risks and issues that are of national concern such as the economy? One contributor is the presence of a national CSIRT. US-CERT is one example.

National CSIRTs identify current threats, vulnerabilities, and adversary tactics to disrupt critical infrastructures. One example is attacking the financial services sector, not only to disrupt services but also to facilitate currency trading for international crime.

CERT's Role and the Importance of Ongoing Research

A key area calling for additional research is the examination of national frameworks to determine how they will work in different countries and cultures, and to examine variations in organizational structures by nation.

CERT is assisting the U.S. Department of Homeland Security in assessing risk for key critical infrastructures, as well as across CIs. One outcome is an estimate of risks based on the threat actor (terrorists, organized crime, industrial espionage, etc.).

CERT looks for insiders working within sectors who may want to destabilize communities. (Refer to Protecting Against Insider Threat podcast for more information about insider threat.)

CERT works with the Committee on Foreign Investment in the U.S. to help assess risks based on foreign investment in U.S. business.

CERT's efforts span the range from governance to operational concerns.

Resources

OECD

ITU

Gulf Cooperation Council

Information Infrastructure Institute (I3P) at Dartmouth University

Partial Listing of Information Sharing and Analysis Centers (ISACs) in the United States

ISAC Council

By sector:

- Electricity Sector ISAC (ES-ISAC)
- Financial Services ISAC (FS-ISAC)
- Food and Agriculture ISAC
- Information Technology ISAC (IT-ISAC)
- Multi-State ISAC (MS-ISAC)
- Surface Transportation ISAC (ST-ISAC)
- Water ISAC

Abele-Wigert, I., Dunn, M. “International CIIP Handbook 2006 (Vol.I): An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies.” Center for Security Studies, ETH Zurich, April 2006.

Anonymous. “(U.S.) National Infrastructure Protection Plan (NIPP).” U.S. Department of Homeland Security, 2006.

Anonymous. “ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: a Management Framework for Organizing National Cybersecurity Efforts.” ITU-D SECRETARIAT DRAFT JANUARY 2008.

Anonymous. “(U.S.) The National Strategy to Secure Cyberspace.” February 2003.

Anonymous. “The Development of Policies for the Protection of Critical Information Infrastructures (CII): A comparative analysis in four OECD countries: Canada, Korea, the United Kingdom and the United States.” Organisation for Economic Co-operation and Development, DSTI/ICCP/REG(2006)15/FINAL, February 2007

Pederson, P., et al. “Critical Infrastructure Interdepency Modeling: A Survey of U.S. and International Research.” Idaho National Laboratory, INL/EXT-06-11464, August 2006.

Suter, M. “A Generic National Framework For Critical Information Infrastructure Protection (CIIP).” Center for Security Studies, ETH Zurich, August 2007.