Data Collection and Incident Analysis: IT-ISAC Perspective

ENISA Workshop

March 17, 2010

Agenda

- IT-ISAC Overview
- ISAC Model with Case Studies (ISAC Initiatives and Conficker)
- Building a Joint Capability

IT-ISAC Mission

- **Share:** Report, exchange and analyze across the IT Sector information on electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures

- **Trust:** Establish a mechanism for systematic and protected exchange and coordination of the Information and trusted collaboration;

- **Lead:** Provide thought leadership to policymakers on cyber security and information sharing issues.

Members

Foundation Members

BAE Systems, IT

CA

Cargill, Inc.

CSC

eBay

EWA, IIT

IBM

Intel Corporation

Microsoft Corp.

Oracle USA, Inc.

SRA International

Symantec Corp.

VeriSign, Inc.

Silver Members

Cisco Systems, Inc.

Juniper Networks

McAfee, Inc.

NeuStar

Bronze Members

Prescient Solutions

USi

IT-ISAC Model

- **Collection:** Members collect, analyze and share. The scope of information in the hands of our members is immense

- **Analysis:** The analytical talent available to the ISAC, through our members, is rich

- **Trust:** The member NDA enables trusted information sharing and collaborative analysis

- **Process:** Con Ops standardizes how we leverage these capabilities

Goals

- **Operating Picture:** Provide a comprehensive view as to threats, vulnerabilities and anomalies

- **Identify New Information Needs:** Supplement current products with information on attacks directed at specific members

- **Company Neutral:** ISAC products represent the collective view of ISAC members, not the views of any company

- **Collaborative Analysis:** By coming together collectively, we’re able to see what we might miss individually

Information Sharing and Correlation

- Emerging Threat Special Interest Group
  - Identify common trends and threats such as third party access to networks, small form factor, distributing threats through non traditional devices.

- Training and Education Initiative
  - Enables subject matter experts to do a deep dive on specific areas of common interest

- International Economic Crime
  - Special Interest Group within the ISAC

Incident Correlation and Analysis: Conficker

- October 2008 Issued first Alert to members and increased Alert levels
- January 2009: Issued bulletin to members
- March-April 2009: Series of focused discussions with members
- Organized cross sector analytical meetings and disseminated IT-ISAC bulletins with additional analytical insight and remediation techniques.

Conficker Lessons

- ISAC Role is to collect, analyze, and distribute products to trusted security partners such as members, other ISACs, government and partner organizations

- Public and policy maker perceptions impact and sometimes drive incident response

- IT-ISAC served as an authoritative, company neutral resource

Building a Joint Capability

- **Cross Sector Coordination**: Integrate the operational capabilities of the federal government, IT and Communications Sectors through co-location and building joint response capabilities.

- **Global Engagement** : Build and strengthen relationships with FIRST, ICASI, and others (ENISA), to build a global capability.

- **Refine Information Needs**: Ensure that we provide relevant and actionable information to our members and partners

IT-ISAC Contact Information:

Scott C. Algeier, Executive Director

salgeier@it-isac.org

703-385-4969--Direct

www.it-isac.org