CYBERSECURITY

RIEMA CONFERENCE
AUGUST 26, 2015

Homeland Security

Cyber Security & Homeland Security:

Preparation, Prevention, and Sustainment Activities for CIKR and SLTT

Michael Leking, CISSP, CISM, PMP

Cyber Security Advisor – Northeast Region
Office of Cybersecurity and Communications (CS&C)
U.S. Department of Homeland Security (DHS)

Office of Cybersecurity and Communications

MISSION:

To enhance the security, resilience, and reliability of the Nation's cyber and communications infrastructure.

Capabilities:

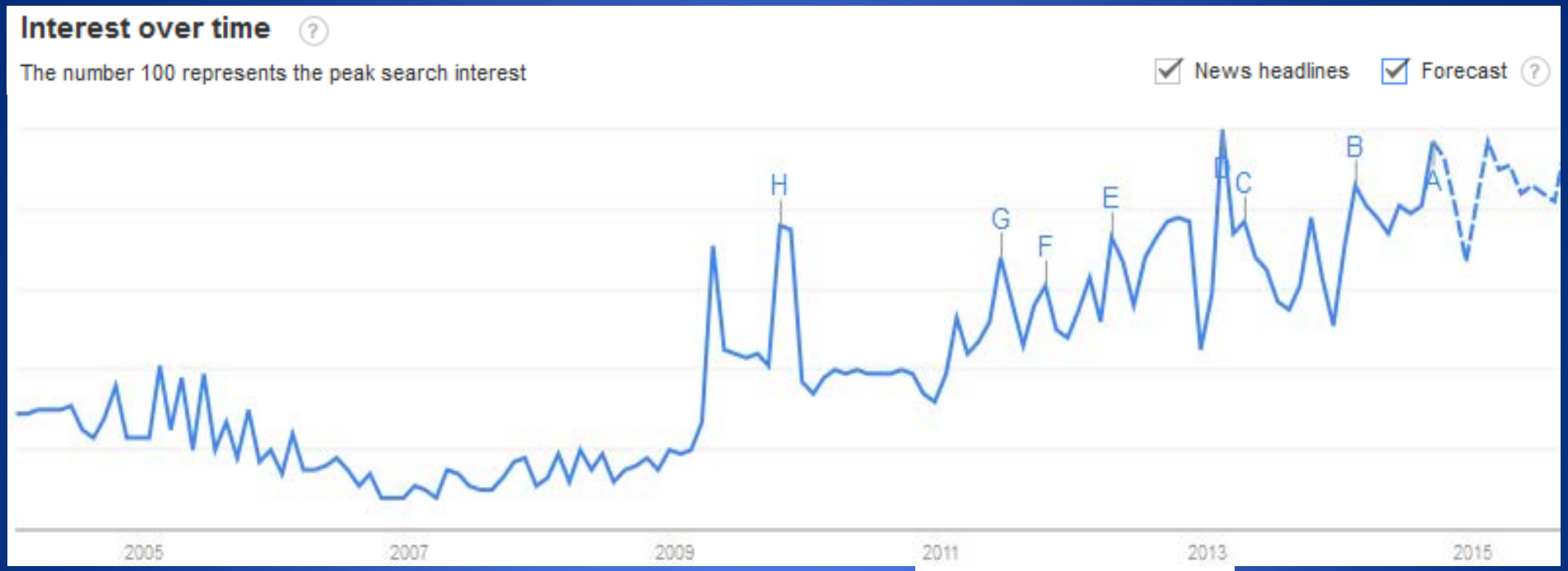
- CS&C works collaboratively with public, private, and international entities to secure, assess, and mitigate cyber risk; and prepare for, prevent, and respond to cyber incidents.
- CS&C leads efforts to protect the federal "**.gov**" domain of civilian government networks and to collaborate with the private sector—the "**.com**" domain—to increase the security of critical networks.
- Build and maintain a world-class organization to advance the Nation's cybersecurity preparedness and raise awareness across the Nation on cybersecurity
- Sector-Specific Agency for the Communications and Information Technology (IT) sectors, CS&C coordinates national-level reporting that is consistent with the National Response Framework (NRF).

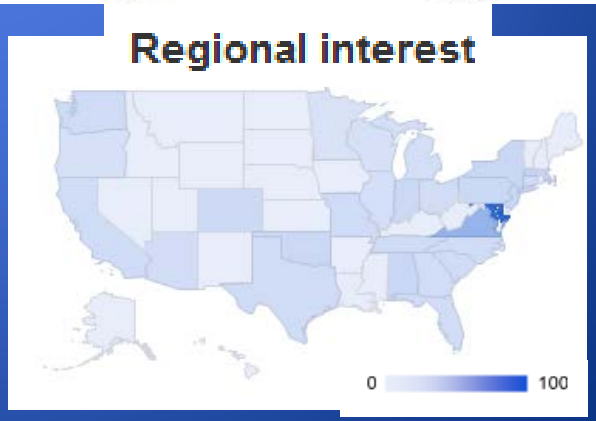
Homeland Security

Why Focus on Cybersecurity & Resilience?

Homeland Security

Google Trends: “Cybersecurity”





Homeland Security

United States Computer Emergency Readiness Team (US-CERT)

Subject Matter Experts in IT Network Architectures

- Networking technologies, malware, digital forensics, enterprise network solutions

State of the Art Advanced Malware Analysis Center (AMAC)

- Analyzes media and/or malware to determine the cause and effect of probable intrusions into critical systems
- Provides indicators to mitigate and prevent future intrusions

Network, System and Host Analysis on Enterprise Systems

- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) Logs
- Proxy and Network Infrastructure Logs
- Network Traffic Analysis
- Disk and Firmware Images

Support for Incident Response, Recovery and Future Defense Efforts

US-CERT Metrics	Fiscal Year 2014
Cyber Incident reports from Remedy	55,523
Number of threat reports via phishing	560,012
On-site response and recovery team deployments	9
Cyber security products – National vulnerability database entries, alerts, bulletins, and other products	7,655
Indicators shared – ECS0	3,156

*Reflects June - September 2013 only

Homeland Security

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

Subject Matter Experts in Industrial Control Systems (ICS)

- Supervisory Control and Data Acquisition (SCADA), Process Control Systems (PCS), Distributed Control Systems (DCS), Remote Terminal Units (RTUs), Human Machine Interfaces (HMIs), Programmable Logic Controllers (PLCs)

Unique Awareness of Emerging Issues and Threats to Control Systems and Vendor Products

State of the Art Analysis Capabilities Specific to ICS that enable –

- Malware and Embedded Systems Analysis
- Patch Testing
- Consequence Analysis

Incident Response Support for ICS-Related Response, Recovery and Future Defense Efforts for Critical Infrastructure

ICS-CERT Metrics	FY 2014
Cyber Incident reports from Federal agencies, critical infrastructure organizations, and international partners	240
On-site technical assistance teams deployed	5
Actionable Critical Infrastructure Security Alerts, bulletins, and other products	243
Unique vulnerabilities affecting ICS products tracked	131
Assessments conducted across critical infrastructure sectors	70
Cyber Security Evaluation Tool (CSET) downloads by critical infrastructure operators	4,826
Number of global public and private partners trained	640

Homeland Security

What are we doing about it?

Homeland Security

Critical Infrastructure Cyber Community (C^3)

Website:

http://www.us-cert.gov/ccubedvp

General C^3 inquiries:

ccubedvp@hq.dhs.gov

- DHS launched the C^3 Program in February, 2014 to complement the launch of the NIST CSF
- The C^3 Voluntary Program helps sectors and organizations that want to use the CSF by connecting them to existing cyber risk management capabilities provided by DHS, other U.S. Government organizations, and the private sector.
- The C^3 website (http://www.us-cert.gov/ccubedvp) describes the various programs DHS offers to critical infrastructure partners, including Federal, State, local, and private sector organizations
- Central location for DHS' cyber risk management resources and tools, including the self-service Cyber Resilience Review (CRR).

Homeland Security

Cybersecurity Tools and Resources

- **C^3 Voluntary Program Small and Midsize Business (SMB) Toolkit**
  - Understanding the Threat Landscape
  - Top Resources for SMB
  - Cybersecurity for Startups
  - C^3 Voluntary Program Outreach & Messaging Kit
  - SMB Leadership Agenda
  - Hands-On Resource Guide

www.us-cert.gov/ccubedvp

- Use the NIST Cybersecurity Framework
- **Take advantage of our**: vulnerability scans, alerts/ bulletins/advisories, training, threat indicators, etc.

Cyber Resilience Review Downloadable Resources

- Self-Assessment Package
  Self-assessment form and report generator.
- Method Description & User Guide
  Walk-through for how an organization can conduct a CRR self-assessment.
- Question Set with Guidance
  Self-assessment question set

Getting Started for Small and Midsize Businesses (SMB)

Cybersecurity is critical to any business enterprise, no matter how small. However, leaders of small and midsize businesses (SMB) often do not know where to begin, given the scope and complexity of the issue in the face of a small staff and limited resources.

To help business leaders get started, DHS has provided a list of top resources specially designed to help SMBs recognize and address their cybersecurity risks.

C³ Voluntary Program SMB Toolkit

This packet contains resources specially designed to help SMBs recognize and address their cybersecurity risks. Resources include talking points for CEOs, steps to start evaluating your cybersecurity program, and a list of hands-on resources available to SMB.

1. Toolkit for Small and Midsize Businesses (SMB) Table of Contents
2. Begin the Conversation: Understanding the Threat Environment
3. Getting Started: Top Resources for SMB
4. Cybersecurity for Startups
5. C³ Voluntary Program Outreach and Messaging Kit
6. SMB Leadership Agenda
7. Hands-On Resource Guide

Stop.Think.Connect. Toolkit

The Stop.Think.Connect.™ campaign has an online Toolkit that includes information specific to SMBs. The Toolkit can be found at http://www.dhs.gov/stopthinkconnect-toolkit or www.stcguide.com.

Small Business Administration (SBA) Training

This 30 minute, self-paced training exercise provides an introduction to securing information in small businesses. For more information, please visit: https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses.

Federal Small Biz Cyber Planner

This tool helps businesses create custom cybersecurity plans. The Small Biz Cyber Planner includes information on cyber insurance, advanced spyware, and how to install protective software. For more information, please visit

DHS' Cyber Security Assessments and Resources

Homeland Security

Cyber Security Evaluation Tool (CSET)®

- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy

CSET Download:

us-cert.gov/control_systems/csetdownload.html

Homeland Security

Cyber Resilience Review (CRR)

- Based on the ***CERT® Resilience Management Model (RMM)***, a process improvement model for managing operational resilience
- Development of CRR methodology began in early 2009
- Deployment across all 18 CIKR sectors as well as State, local, tribal, and territorial governments
- **Primary goal:** Evaluate how CIKR providers manage cyber security of significant information services and assets (information, technology, facilities, and personnel)
- **Secondary goal:** Identify opportunities for improvement in cyber security management and reduce operational risks related to cyber security

Homeland Security

CRR Self-Assessment Package

- Released in February 2014 to complement the launch of the NIST CSF.
- The CRR Self-Assessment Kit allows organizations to conduct a review without outside facilitation.
- Contains the same questions, scoring, and reporting as the facilitated assessment.
- The kit contains the following resources:
  - Method Description and User Guide
  - Complete CRR Question Set with Guidance
  - Self-Assessment Package (automated toolset)
  - CRR to NIST CSF Crosswalk
- **CRR Self-Assessment Kit website:** http://www.us-cert.gov/ccubedvp/self-service-crr

Homeland Security

Homeland Security

Contact Information

Michael Leking (michael.leking@dhs.gov)

Cyber Security Advisor - Northeast Region

Office of Cybersecurity and Communications

Department of Homeland Security

Rhode Island State Fusion Center

John Soscia
Senior Intelligence Analyst

WHAT IS A FUSION CENTER?

- A central location where intelligence information (primarily concerning homeland security) is collected, processed, analyzed and disseminated to partners and those who would benefit including but nor limited to; law enforcement, public safety, emergency management, private sector, etc.

- The Fusion Center concept has been expanded to incorporate all crimes in addition to anti-terrorism efforts such as narcotics trends, organized crime, outlaw motorcycle gangs, street gangs, etc. It has also expanded to cover all hazards.

Why were Fusion Centers created?

- The events leading up to the attacks on Twin Towers on 9/11 were studied by the 9/11 Commission
- One of the strongest recommendations was to improve Intelligence sharing among law enforcement
- At the time of the attacks, credible intelligence concerning a potential terrorist plot had been collected, but was not shared with other law enforcement agencies
- Antiquated databases controlled by various agencies contained information that was restricted within the agency due to security policies and a lack of technology

Rhode Island State Fusion Center

What is the function of the RI State Fusion Center ?

- Access and monitor a wide array of information and intelligence, as well as a wide array of data bases within law enforcement.

- Analyze the information received in comparison to trends being observed in other states and countries.

- Disseminate in a timely and concise manner to the individuals who will benefit from the information.

FUSION CENTER OVERVIEW

- Outreach conducted Fusion Center/Terrorism training for RI State Police Academy, RI Municipal Police Academy, RI Sheriffs, RIPCA, RIDA, RIFA, RILETA, Firefighter Associations, Hospital Association, EMA Directors, DOH, Retail Assn.'s
- Attend training, conferences and intelligence sharing forums throughout the Country
- Provide analytical products for investigations
- Create and disseminate Intelligence bulletins
- Special Event planning and support (examples: Tall Ships, USN International Sea Power Symposium, Bristol Parade, Air Show, America's Cup)

FUSION CENTER OVERVIEW

- Four full time RISP Detectives (1 assigned to JTTF)
- Four full time RISP Analysts (all retired police officers)
- DHS Intelligence Officer
- RIEMA personnel detailed full time (CI/KR)
- Minimum of 3 POC's for every law enforcement agency in RI
- Liaisons with numerous federal and state agencies
- Co-located with the Providence RA of the FBI and the JTTF
- Increased contact and working relationship with the private sector
  - Exploring the potential for partners from the private sector to work in the Fusion Center on a part-time basis

Sample List of Partners

- All local law enforcement
- FBI
- DHS
- ATF
- USSS
- TSA
- DEA
- HSI / ICE
- US Marshals
- Dept. of State
- Interpol
- ATAC
- Department of Health
- Campus Security
- National Network of FCs
- National Guard
- NCIS DoD
- US Coast Guard
- US Postal Inspectors
- Fire / Arson Investigators
- Amtrak
- RIEMA
- Private Sector
- Private Security
- Hotel Network
- Hospitals
- Banking/Finance Sector
- All CIKR sectors

Private Sector Component

- *Operation Safe-RI:*

  Outreach to private businesses to include storage facilities, car rental companies, insurance companies, chemical companies, State Agencies, hospitals, hotels, private transit, etc.
- Provide contact information to these businesses in the event suspicious activity is observed
- Include input from private security and investigators

Private Sector Component

How can fusion centers and the private sector be mutually beneficial to each other?:

- Shared resources
- Access to information
- Access to SME's
- Access to resources in other States
- Robust national network of fusion centers
- Increased need for information sharing, especially in the cyber realm

Sources of Information

- Review of intelligence and informational bulletins from across the Country and the World
- Web and telephonic chats and conferences
- Intelligence sharing websites
- Local input/output
- Private Sector input (result of outreach programs)

All Partners

Critical Infrastructure

Privately owned Critical Infrastructure

- 85-90%
- What intelligence are they entitled to, what portion of their information are we entitled to?
- What are the consequences of including or not including the Private Critical Infrastructure?
- What can be shared, how can it be protected?
- How to pass on intelligence or information?:
  - Clearance issue
  - What can/should they do with it?

“See Something, Say Something”

- Department of Homeland Security (DHS)

  "If You See Something, Say Something, <u>DO SOMETHING</u>"

- Creates initiative between DHS and the American public to play an active role in ensuring the safety and security of our nation

- If something seems or looks suspicious or out of the ordinary, report it to the appropriate authority

Rhode Island State Fusion Center

401-444-1117

TIPS: 866-490-8477

FAX: 401-458-1173

Email: fusion@risp.dps.ri.gov

Website: http://www.fusioncenter.ri.gov/

QUESTIONS?