

March 2014



Homeland
Security

Homeland Security Lessons

Learned:

An Analysis from Cyber Security Evaluations

Bradford J. Willke, CISSP

Program Manager, Cyber Security Advisor Program
Office of Cybersecurity and Communications (CS&C)
National Protection and Programs Directorate (NPPD)

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**

Cyber Security Advisors (CSA)

Roles and Responsibilities

- Raise awareness of CS&C activities
- Assist in identification of critical cyber / information infrastructures supporting CI/KR, and interdependencies
- Coordinate and lead cyber security evaluations of critical infrastructure
- Function as a regional CS&C advisor to planning, operational, and strategic cyber security efforts and communities-of-interest –private and public sector
- Establish working relationship and rapport with homeland security officials and cyber security principals within homeland security, IT operations, and emergency management agencies
- Coordinate with Federal personnel within region to integrate cyber preparedness, strategic communications, incident response, and evaluations (i.e., PSAs, FEMA, Federal LE – FBI, USSS, etc)
- Coordinate strategic outreach and collect strategic requirements – to promote CS&C operational enhancements and policy initiatives



Critical Infrastructure Cyber Community (C³)

Website:

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

General C3 inquiries:

ccubedvp@hq.dhs.gov

C3 VP (Pre-Recorded) Webinar:

<https://share.dhs.gov/p4k4bp51kx7/>

- DHS launched the C³ Program in February 2014 to complement the launch of the NIST CSF
- The C³ 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 C3 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
- Many of the programs described on the following slides can also be found on the website



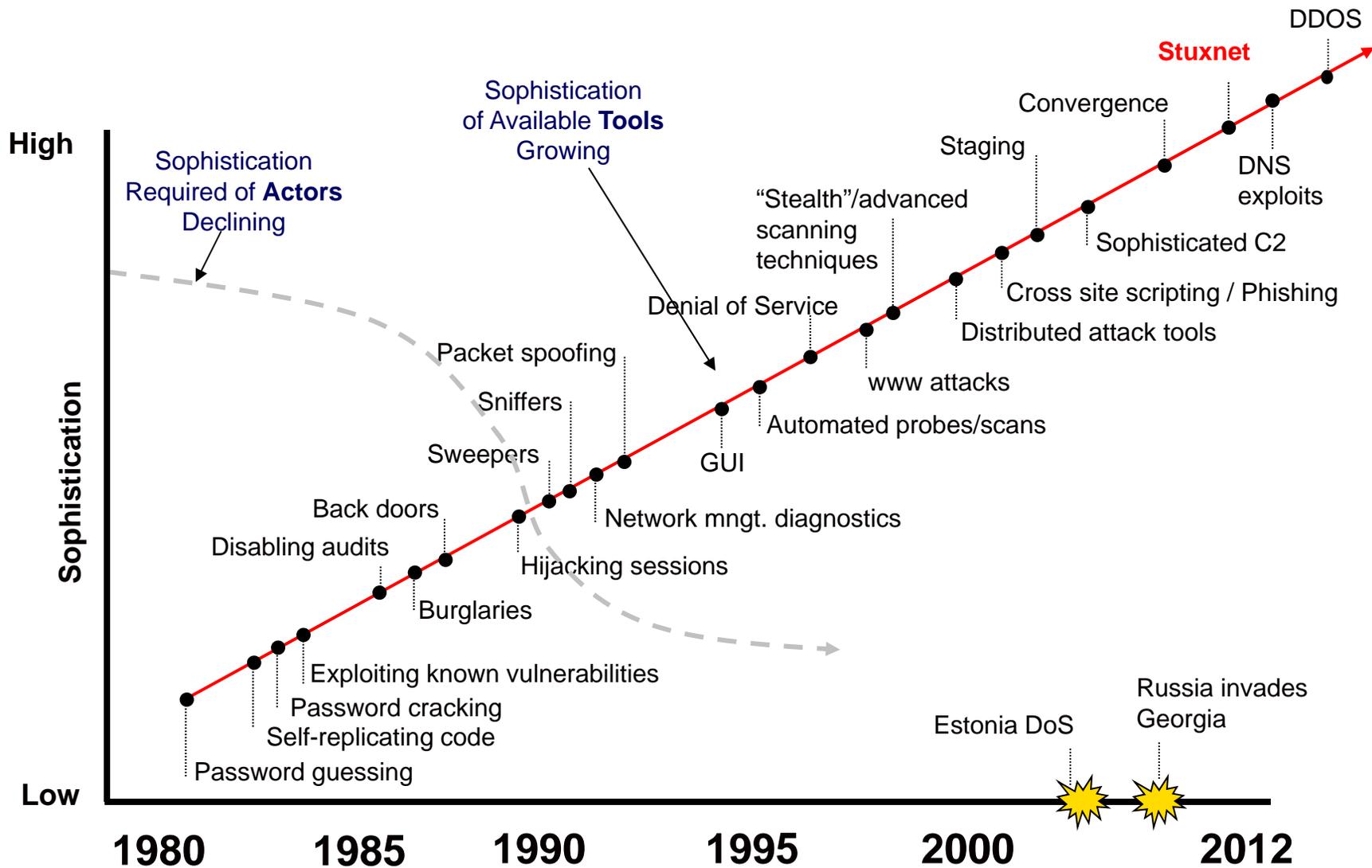
**Homeland
Security**

CYBER THREAT TRENDS AND SPECIFIC ATTACKS



**Homeland
Security**

Growth of Cyber Threats



Homeland Security

Cyber Threat: Human Threats

Who is behind these intentional threats?



- Insider Threat
 - Insiders have a unique advantage due to access/trust
 - They can be motivated by revenge, organizational disputes, personal problems, boredom, curiosity, or to “prove a point”



- Malware Authors
 - Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware



- Phishers
 - Individuals, or small groups who attempt to steal identities or information for monetary gain



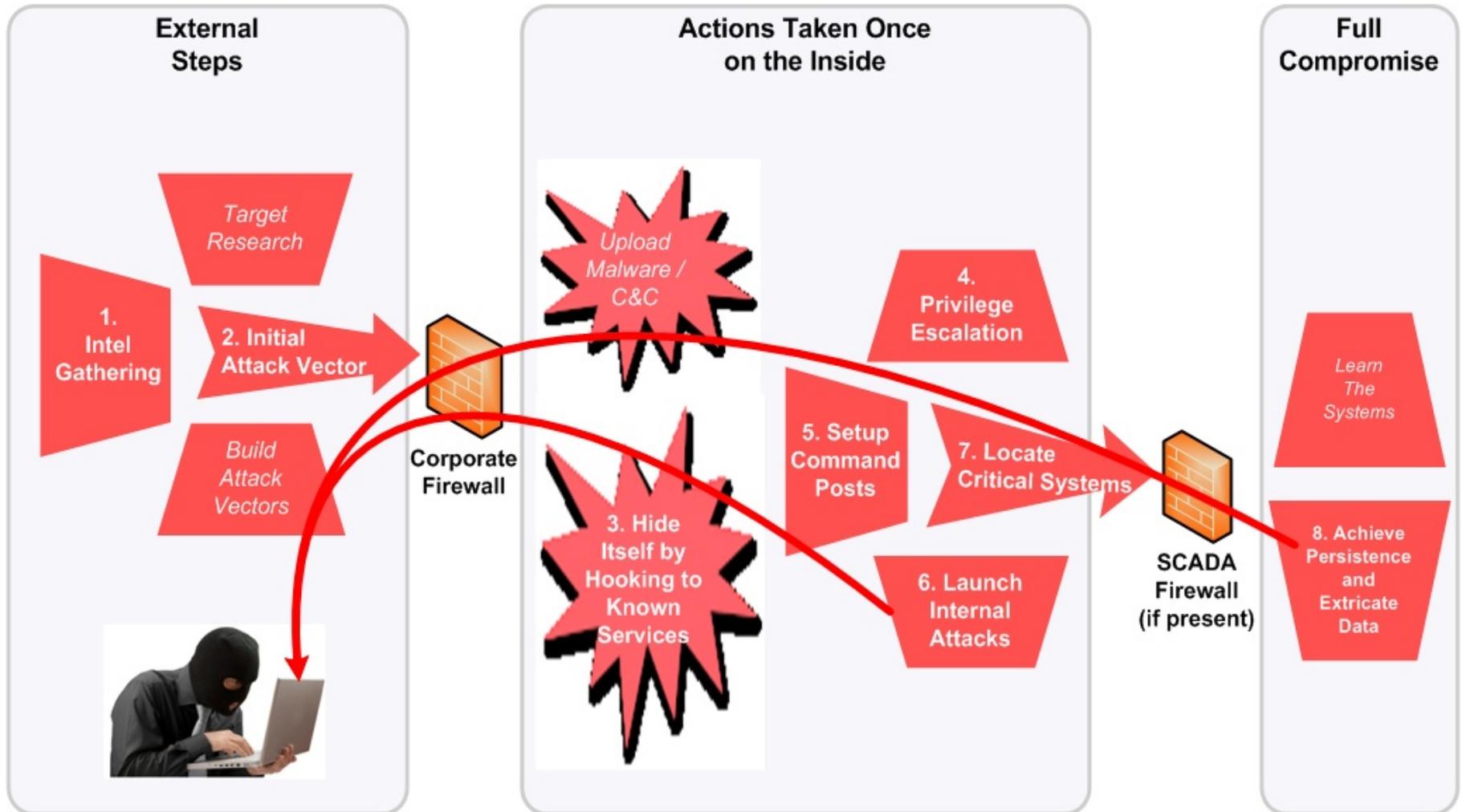
- Spammers
 - Individuals or organizations who distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations

- Terrorists
 - Cyber attacks have the potential to cripple unsecured infrastructures
 - Cyber-linkages between sectors raise the risk of cascading failure



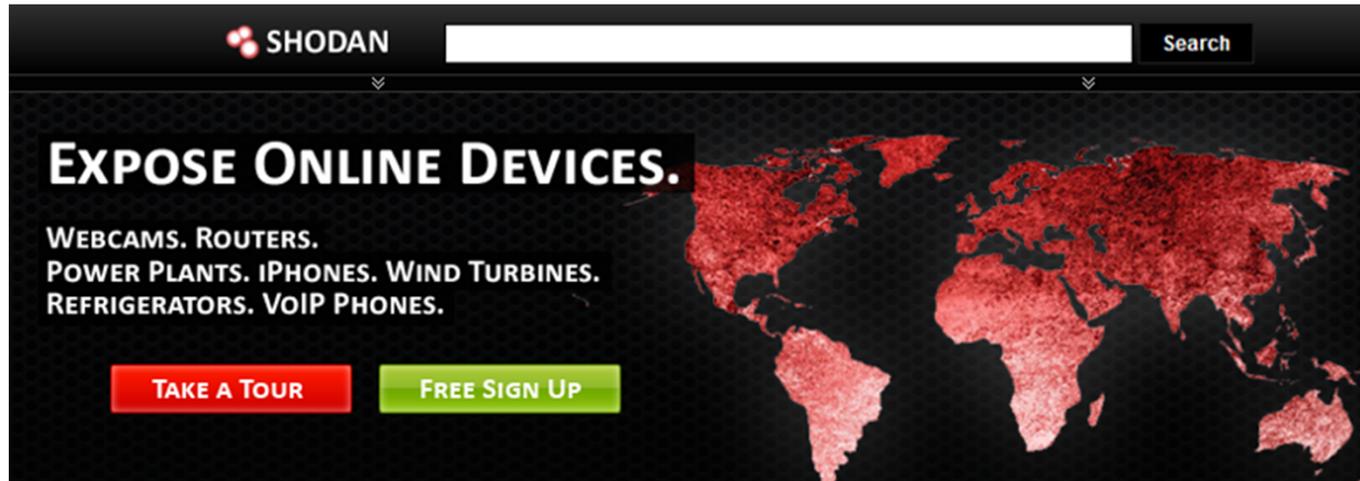
Homeland
Security

Cyber Attack: Step by Step



Homeland Security

ShodanHQ



- ShodanHQ is the first search engine designed to search for computers and devices.
- *Recommendation: Run a search using your network IP range to identify or validate: devices, misconfigurations, location, services, HW/SW versions, etc.*
- ShodanHQ has identified:
 - **~500,000** devices connected to the internet
 - **98,415** were located in the U.S.
 - **7,257** were associated with Industrial Control Systems



Homeland
Security

2012: Targeted cyber attack on pipelines

- **Over 20 targeted pipeline** operators (December 2011 – June 2012)
- **Confirmed intrusions** and near misses
- Adversary is targeting industrial control systems information
 - Document searches: “SCAD*”
 - Personnel Lists
 - Usernames/Passwords
 - Dial-Up access information
 - System manuals
 - Exfiltrated ICS access credentials
- The data exfiltrated could provide an adversary with the capability to access US ONG ICS including performing unauthorized operations



What was taken?

- All_gate_meter.xls
- <station>_SCADA 8-23-2002.vsd
- Contact List Gas Scada.xls
- <redacted>_Area_RTUs.xls
- **Dial Up ##### Vector Lists.xls**
- SCADA_Server_UsersGuide.pdf
- Gas Control Numbers.xls
- Gas SCADA Profiles Defined 10-22-03.xls
- Gas-Control Asset list.xls
- **<station> Dialup.xls**
- PASS1.xls
- <station> datapoints for log.xls
- RTU point list.xls
- **RTU SITES.xls**
- SCADA Division Options.ppt
- SCADA HARDWARE UPGRADE.ppt
- SCADA Sites.xls
- Scada Users Manual.zip
- **SCADA_logons.doc**
- **Security.zip**
- Standard Colors & Symbols.xls
- Station Control Testing Procedures.ppt
- **DIALUP.DOC**
- DISPLAYS.DOC
- <station> Comm Card Converter pinout.pdf
- Comm Ports for Airlink.pdf
- D-Sub to RJ45 Modular Adapters.pdf
- **SCADA Personnel.html**



A Wide Range of Offerings for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
 - US-CERT Operations Center
 - Remote and On-Site Assistance
 - Malware Analysis
 - Incident Response Teams
 - ICS-CERT Operations Center
 - ICS-CERT Malware Lab
 - Cyber Security Evaluation Tool
 - Incident Response Teams
 - NCATS
 - Cyber Hygiene service
 - Risk and Vulnerability Assessment
- US-CERT
 - National Cyber Awareness System
 - Vulnerability Notes Database
 - Security Publications
- Control Systems Security Program
 - Cybersecurity Training
 - Information Products and Recommended Practices
- Cyber Exercise Program
- Cyber Security Evaluations Program
 - Cyber Resilience Review
 - Cyber Infrastructure Survey Tool



**Homeland
Security**

DHS Cyber Security Evaluations

- **Cyber Hygiene (CH) Evaluation**
- **Pen Test (*aka* RVA)**
- **Cyber Resilience Review (CRR)**
- **Cyber Security Evaluation Tool (CSET)**

Other Evaluations:

- **Cyber Infrastructure Survey Tool (C-IST)**
- **Supply Chain Risk Management (SCRM) Assessment**
- **ICS Design Architecture Review**
- **ICS Network Analysis Verification & Validation**



**Homeland
Security**

CYBER HYGIENE (CH)

Overview:

Cyber hygiene (CH) refers to steps that computer users can take to improve their cybersecurity and better protect themselves online. It may include reorganizing the IT infrastructure, hardware and devices; patching authorized software and removing unauthorized software; continuous monitoring, training and awareness; and formalizing existing informal information security controls.

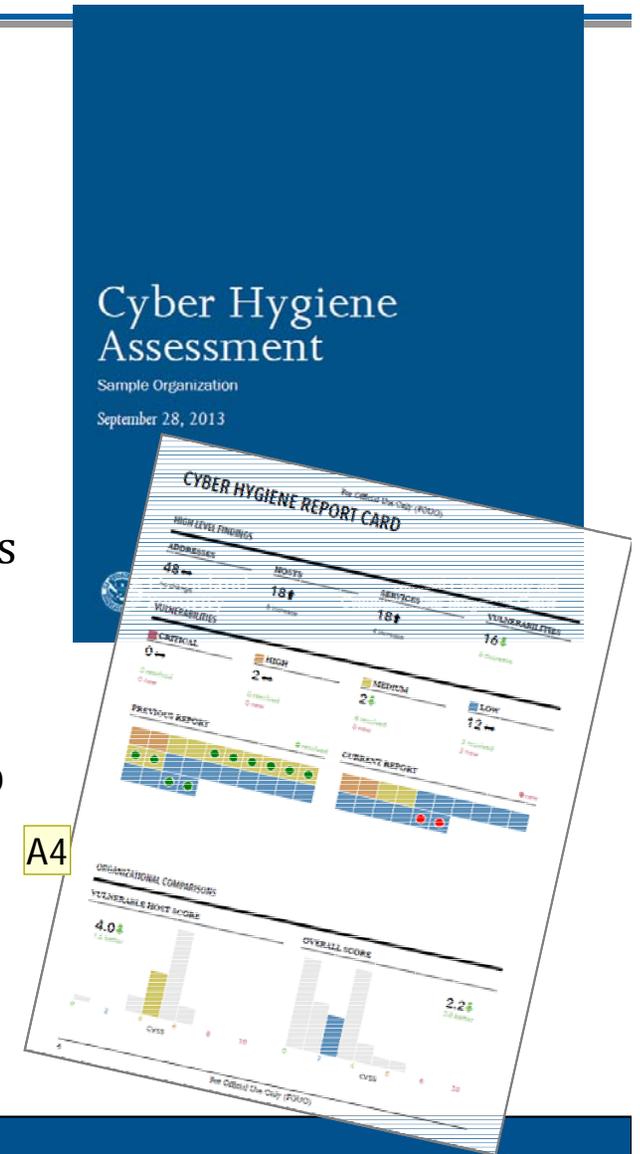


**Homeland
Security**

FOUO / UNCLASS

Cyber Hygiene

- Assess Internet accessible systems for known vulnerabilities and configuration errors.
- Work with organization to proactively mitigate threats and risks to systems. Activities include:
 - **Network Mapping**
 - Identify public IP address space
 - Identify hosts that are active on IP address space
 - Determine the O/S and Services running
 - Re-run scans to determine any changes
 - Graphically represent address space on a map
 - **Network Vulnerability & Configuration Scanning**
 - Identify network vulnerabilities and weakness



Slide 15

A4

Reomved the DNSSEC language as right now it is a manual process and we have a difficult time doing 140 Federal agenices.

Author, 12/18/2013

PENETRATION TESTS (AKA NETWORK RISK AND VULNERABILITY ASSESSMENTS)

Overview:

A penetration test, or the short form pentest, is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.

The process involves identifying the target systems and the goal, then reviewing the information available and undertaking available means to attain the goal. A penetration test target may be a white box (where all background and system information is provided) or black box (where only basic or no information is provided except the company name). A penetration test will advise if a system is vulnerable to attack, if the defenses were sufficient and which defenses (if any) were defeated in the penetration test.



**Homeland
Security**

FOUO / UNCLASS

Risk and Vulnerability Assessment (RVA)

- Conducts red-team assessments and provides remediation recommendations.
 - Identify risks, and provide risk mitigation and remediation strategies
 - Improves an agency's cybersecurity posture, limits exposure, reduces rates of exploitation, and increases the speed and effectiveness of future cyber attack responses.
- Services Include:

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness or test responses in systems, applications, network and security controls
Social Engineering	Crafted e-mail at targeted audience to test Security Awareness / Used as an attack sector to internal network
Wireless Discovery & Identification	Identify wireless signals (to include identification of rogue wireless devices) and exploit access points
Web Application Scanning and Testing	Identify web application vulnerabilities
Database Scanning	Security Scan of database settings and controls
Operating System Scanning	Security Scan of Operating System to do Compliance Checks



CYBER RESILIENCE REVIEW (CRR)

Overview:

The Cyber Security Evaluation Program (CSEP), within the Department of Homeland Security's (DHS) National Cyber Security Division (NCSD), conducts a no-cost, voluntary Cyber Resilience Review (CRR) to evaluate and enhance cyber security capacities and capabilities within all 16 Critical Infrastructure and Key Resources (CIKR) Sectors, as well as State, Local, Tribal, and Territorial (SLTT) governments. The CRR seeks to understand cyber security management of services (and associated assets) critical for an organization's mission success by focusing on protection and sustainment practices within ten key domains that contribute to the overall cyber resilience of an organization.



**Homeland
Security**

FOUO / UNCLASS

Cyber Resilience Review (CRR)

- One-day, no-cost, facilitated cyber security evaluation
- Deployment across all 16 CIKR sectors as well as State, local, tribal, and territorial governments
- Based on the *CERT® Resilience Management Model (RMM)*, a process improvement model for managing operational resilience
- **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

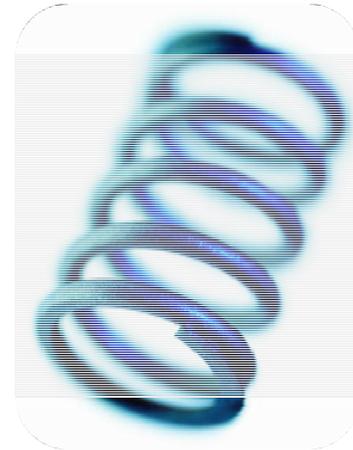


**Homeland
Security**

FOUO / UNCLASS

Cyber Resilience

- **Definition:**
 - The ability of an organization to continue vital IT services and information management functions in a less-than-ideal situation while reacting and adapting to stresses



Protect (Security)	Sustain (Continuity)
Perform (Capability)	Repeat (Maturity)



CRR Domains

- These represent key areas that typically contribute to an organization’s cyber resilience— each domain focuses on:
 - **Documentation** in place, and periodically reviewed & updated
 - **Communication & notification** to all those who need to know
 - **Execution/Implementation & analysis** in a consistent, repeatable manner
 - **Alignment** of goals and practices within & across CRR domains

AM	Asset Management <i>identify, document, and manage assets during their life cycle</i>	SCM	Service Continuity Management <i>ensure continuity of IT operations in the event of disruptions</i>
CCM	Configuration and Change Management <i>ensure the integrity of IT systems and networks</i>	RISK	Risk Management <i>identify, analyze, and mitigate risks to services and IT assets</i>
CNTL	Controls Management <i>identify, analyze, and manage IT and security controls</i>	EXD	External Dependency Management <i>manage IT, security, contractual, and organizational controls that are dependent on the actions of external entities</i>
VM	Vulnerability Management <i>identify, analyze, and manage vulnerabilities</i>	TRNG	Training and Awareness <i>promote awareness and develop skills and knowledge</i>
IM	Incident Management <i>identify and analyze IT events, detect cyber security incidents, and determine an organizational response</i>	SA	Situational Awareness <i>actively discover and analyze information related to immediate operational stability and security</i>



Maturity Not Just Capability

- A MIL (Maturity Indicator Level) measures *process institutionalization*, and describes attributes indicative of mature capabilities.

MIL Level 5 – Defined

All practices are performed (MIL-1); planned (MIL-2); managed (MIL-3); measured (MIL-4); and consistent across all internal constituencies who have a vested interest— processes/practices are defined by the organization and tailored by organizational units for their use, and supported by improvement information shared amongst organizational units.

MIL Level 4 – Measured

All practices are performed (MIL-1); planned (MIL-2); managed (MIL-3); and periodically evaluated for effectiveness, monitored & controlled, evaluated against its practice description & plan, and reviewed with higher-level management.

MIL Level 3 – Managed

All practices are performed (MIL-1); planned (MIL-2); and governed by the organization, appropriately staffed/funded, assigned to staff who are responsible/accountable & adequately trained, produces expected work products, placed under appropriate configuration control, and managed for risk.

MIL Level 2 – Planned

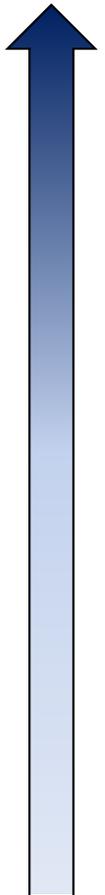
All practices are performed (MIL-1); and established, planned, supported by stakeholders, standards and guidelines.

MIL Level 1 – Performed

All practices are performed, and there is sufficient and substantial support for the existence of the practices.

MIL Level 0 – Incomplete

Practices are not being performed, or incompletely performed.



Cyber Resilience Reviews (CRR)

- A no-cost, voluntary, interview-based review producing a formal report
 - Takes one (1) day (i.e., 5-6 hours excluding lunch and breaks) to complete
- Helps CIKR and SLTT partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk during:
 - normal operations (i.e., protection & sustainment)
 - times of operational stress and crisis (i.e., survivability & resilience)
- Based on the CERT ® Resilience Management Model (CERT® RMM), a process improvement model for managing operational resilience
 - Cross-referenced and compatible with the NIST Security Management Framework (i.e., EO 13636)
- Information provided during the CRR is afforded protection under the DHS Protected Critical Infrastructure Information Program
- Scheduling or general inquiries to: CSE@hq.dhs.gov
 - Sean McCloskey (sean.mccloskey@hq.dhs.gov), Program Manager, Cyber Security Evaluations



**Homeland
Security**

FOUO / UNCLASS

CYBER SECURITY EVALUATION TOOL (CSET)

Overview:

The Cyber Security Evaluation Tool (CSET®) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS Industrial Control System Cyber Emergency Response Team (ICS-CERT) by cybersecurity experts and with assistance from the National Institute of Standards and Technology (NIST). This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.

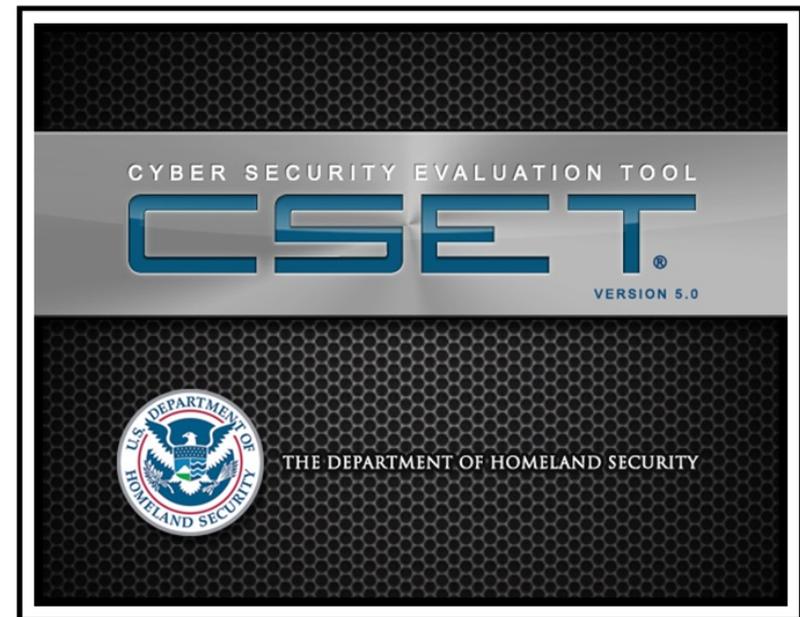


**Homeland
Security**

FOUO / UNCLASS

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:

http://us-cert.gov/control_systems/csetdownload.html



**Homeland
Security**

FOUO / UNCLASS

CSET® Standards

Requirements Derived from Widely Recognized Standards

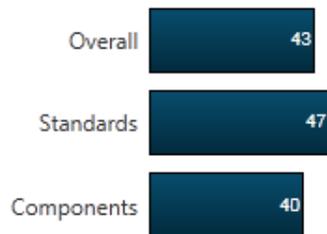
NIST Special Publication 800-53	Recommended Security Controls for Federal Information Systems Rev 3 and with Appendix I, ICS Controls
TSA Pipeline Security Guidelines	Transportation Security Administration (TSA) Pipeline Security Guidelines, April 2011
NERC Critical Infrastructure Protection (CIP)	Reliability Standards CIP-002 through CIP-009, Revisions 2 and 3
DoD Instruction 8500.2	Information Assurance Implementation, February 6, 2003
NIST Special Publication 800-82	Guide to Industrial Control Systems (ICS) Security, June, 2011
NRC Reg. Guide 5.71	Cyber Security Programs for Nuclear Facilities, January 2010
CFATS RBPS 8- Cyber	Chemical Facilities Anti-Terrorism Standard, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27
DHS Catalog of Recommendations	DHS Catalog of Control Systems Security, Recommendations for Standards Developers, Versions 6 and 7



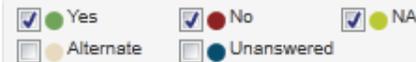
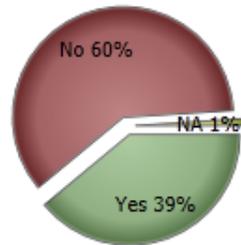
**Homeland
Security**

FOUO / UNCLASS

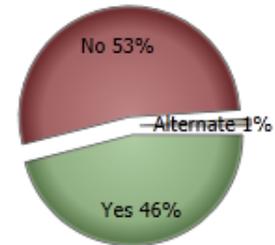
Assessment Compliance



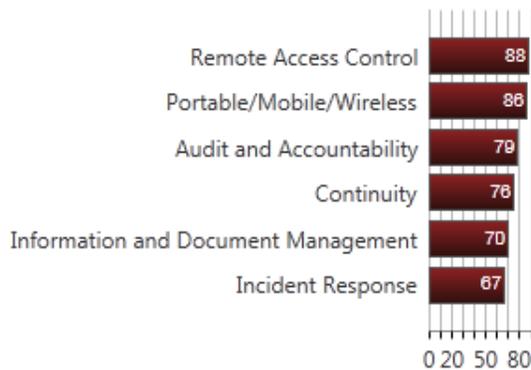
Components Summary Results



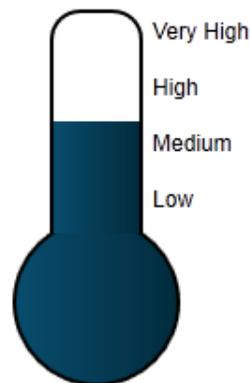
Standards Answers Summary



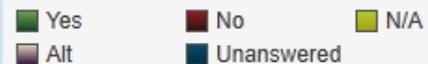
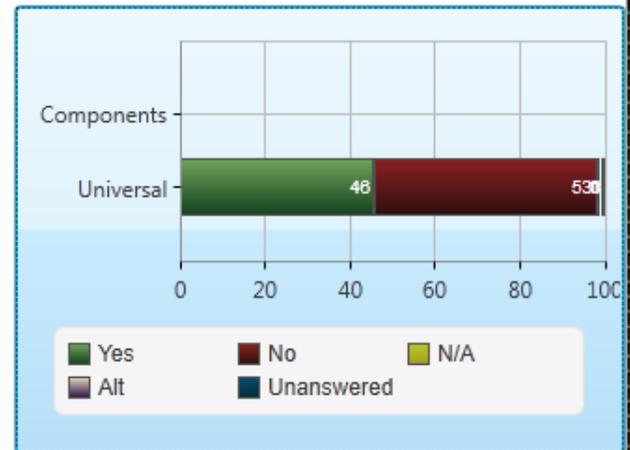
Standards Top Categories of Concern



Security Assurance Level:



Summary of Results by Selected Standards



DOCUMENT LIBRARY

CSET Main Window

File Windows Help

CSET

INFORMATION STANDARDS DIAGRAM QUESTIONS ANALYSIS REPORTS RESOURCE LIBRARY

Tools Diagram Drawing Format

South Creek Processing Plant

The diagram illustrates the network architecture for the South Creek Processing Plant. It is divided into three main sections:

- Corporate Network (Yellow background):** Includes a Web server (Web_81), an External network (Extern...), an ID-786 device, and Remote/Public connections (Remot..., Publo...).
- Control System (Light Blue background):** A central hub connecting to an SCADA Firewall, Operator workstation, Server A, Server B, Historian, Gateway PLC, and three PLCs (PLC 1, PLC 2, PLC 3). It also shows various hardware like NP-2342, LE-3432, MO-3898, and EW-808.
- Control System (Light Blue background):** A detailed view of a control system including a Router, Intern... (Internal network), Switch C-322, and various hardware components like WE 8-34242, A8-4343, VP-77C8, W-EKD22, DB 3-8888, T8-3636, 88-0002, MTU-43242, CK-8832, RTU-32423, IED_2342, DC8-4324, FEP-34342, and HH-4343.

DIAGRAM SYMBOLS

DOCUMENT LIBRARY

DIAGRAM PROPERTIES

FOUO / UNCLASS

STANDARDS PREVIOUS NEXT QUESTIONS

Hard-copy Reports

SITE SUMMARY REPORT

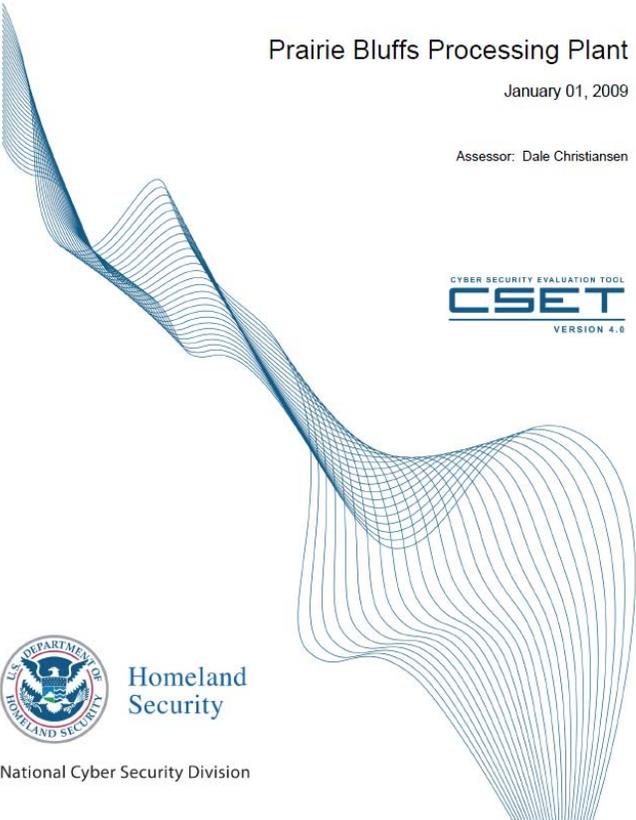
CONTROL SYSTEMS CYBER SECURITY EVALUATION

Prairie Bluffs Processing Plant

January 01, 2009

Assessor: Dale Christiansen







Homeland Security

National Cyber Security Division

PAGE 1

CYBER SECURITY EVALUATION

DESCRIPTION OF ASSESSMENT

This report presents the results of a cyber security assessment performed using the Cyber Security Evaluation Tool (CSET), a stand alone, desktop software application developed for the U.S. Department of Homeland Security (DHS). Before generating this report, the assessor was presented with a list of recognized industrial and governmental standards, guidelines, and best practices. A series of requirements-based questions were generated for each selected standard. If a network topology diagram was created, component-specific questions were also generated. The tool then combined the answered questions with encoded weights and ranking values to determine the facility's cyber security posture.

EXECUTIVE SUMMARY

Cyber terrorism is a real and growing threat. Standards and guides have been developed, vetted, and widely accepted to assist with protection from cyber attacks. The Cyber Security Evaluation Tool (CSET) includes a selectable array of these standards for a tailored assessment of cyber vulnerabilities. Once the standards were selected and the resulting question sets answered, the CSET created a compliance summary, compiled variance statistics, ranked top areas of concern, and generated security recommendations.

The compliance summary charts below provide a high level overview of assessment results. The Summary Percent Compliance chart shows overall security status as well as a breakdown between compliance to selected standards (known as administrative) and compliance of those components depicted on the network diagram. The next two sets of graphs provide greater detail on administrative and component compliance.

The Evaluation Against Selected Standards and Question Sets looks at just the responses to the standards selected at the start of the assessment. The Standards Variance pie chart shows a combined compliance picture while the bar chart shows compliance by security topic. One hundred percent represents full compliance. The Analysis of Network Components is similar but presents results for the component diagram. The Combined Component Variance pie chart shows the overall compliance of all components and the bar chart shows compliance by component type.

The Areas of Concern - Top Subject and Question section lists the five areas of greatest vulnerability. Addressing these areas quickly will provide the greatest return on investment.

SUMMARY PERCENT COMPLIANCE

Overall	39%
Administrative	52%
Components	37%

CSET

RESOURCE LIBRARY

Document Tree Search

- ▶ Guidance
- ▶ Reports
- ▲ Templates
 - ▶ Cryptography & Encryption
 - ▶ Processes & Procedures
 - ▶ Access Control
 - ▶ Service Providers
 - ▶ Wireless
 - ▶ Incidents
 - ▲ Security Plans
 - ▶ Contingency Plan_IT-HHS Template
 - ▶ CyberSec Plan-NRC Template
 - ▶ IT Disaster Recovery Plan-FLA Template
 - ▶ InfoSec Plan-AbqSPIN Template
 - ▶ InfoSec ISS-Neb Template
 - ▶ Sec Approach Plan-HHS Template
 - ▶ SecPlan-CoSN Template
 - ▶ SecPlan_Major Apps-USG Template
 - ▶ SecPlan-LMRs-PSWN Template
 - ▶ SecPlan_Network-QIT Template
 - ▶ SSP-HHS Template
 - ▶ SSP-Mod Impact-NIST Template
 - ▶ Lab Policy Template-SANS
 - ▶ Nuclear
 - ▶ Access control
 - ▶ Test & Evaluation
 - ▶ Servers
 - ▶ Communications
- ▶ Standards
- ▶ Cyber Security Procurement Language
- ▶ Catalog of Recommendations



This library of cyber security standards, reports, and templates are provided for your convenience. Additionally there are several cyber security guides and white papers to assist you in gaining a general background in cyber security, determining priorities, or specific helps. Specific helps include white papers and instructions on securing network components such as a firewall or web server.

Library documents may be browsed using the "Document Tree" tab on the left side of the screen. Documents are grouped by type and topic. If you are looking for a specific document a keyword or title search may also be performed using the "Search" tab in the left pane. Clicking on a document title link in the left-hand pane displays the document. To save a document to your local hard drive click the export button.

FOUO / UNCLASS

DHS EVALUATION FINDINGS & LESSONS-LEARNED



**Homeland
Security**

Data Points: 2011 Nationwide Cyber Security Review

Strengths:

- 52% have implemented and/or validated protective measures for the detection and removal of malicious code
- 81% of all respondents have adopted cyber security control frameworks and/or security methodologies
- 42% have implemented and/or validated logical access controls (e.g., termination/transfer procedures, ACLs, remote access)

Weaknesses:

- 42% of respondents stated they do not have independent testing and/or audit program established
- 45% of respondents stated they have not implemented a formal risk management program (e.g., risk assessments, security categorization)
- 46% of respondents stated they have not implemented Monitoring and Audit Trails which is important to determine if an incident is occurring or has occurred.
- 31% of all respondents have never performed a contingency exercise
- 67% of all respondents stated it has been at least two years since they updated their Information Security Plan
- 66% of all respondents stated it has been at least two years since they updated their Disaster Recovery Plans

10	Security within Technology Lifecycle
11	Risk Management
12	Monitoring and Audit Trails

These results are based on the 162 resp



Homeland Security

FOUO / UNCLASS

DHS CRR Analytical Findings

- From an analysis of a total of 115 organizations in 43 states across 12 sectors participating in evaluations of cyber security management and operational practices in Critical Infrastructures / Key Resources (CIKR), DHS found:

Only 14% of organizations have a documented plan for performing situational awareness activities.

A majority (70%) of organizations do not have a documented risk management plan.

Less than half of organizations identify control objectives, and worse yet less than half of those that do actually implement security control to meet those objectives

55% to 65% of organizations have not developed a strategy to guide their vulnerability management effort.

A majority (65%) of organizations lack a process to escalate and resolve incidents.

50% of organizations do not have a formal strategy to ensure continuity of the critical service, and even fewer (<40%) execute a formal test of these continuity plans.

Nearly half of the organizations assessed do not document which assets support critical services.

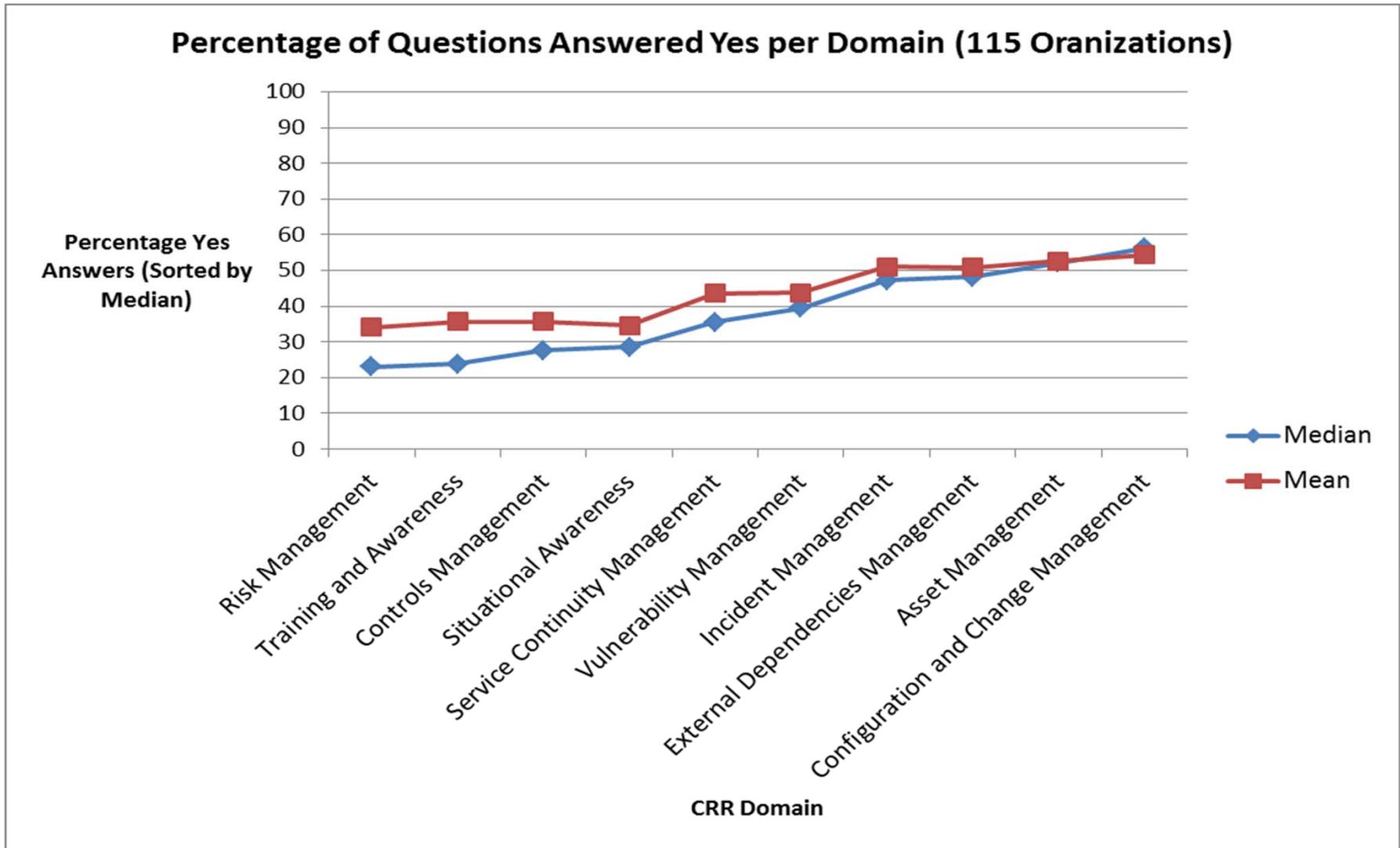
A large majority (>80%) of organizations identify external dependencies, but nearly half fail to identify risks associated with these dependencies.

Source: U.S. Department of Homeland Security. *Cyber Resilience Review Data Analysis*. Office of Cybersecurity and Communications. Washington: September 2013.

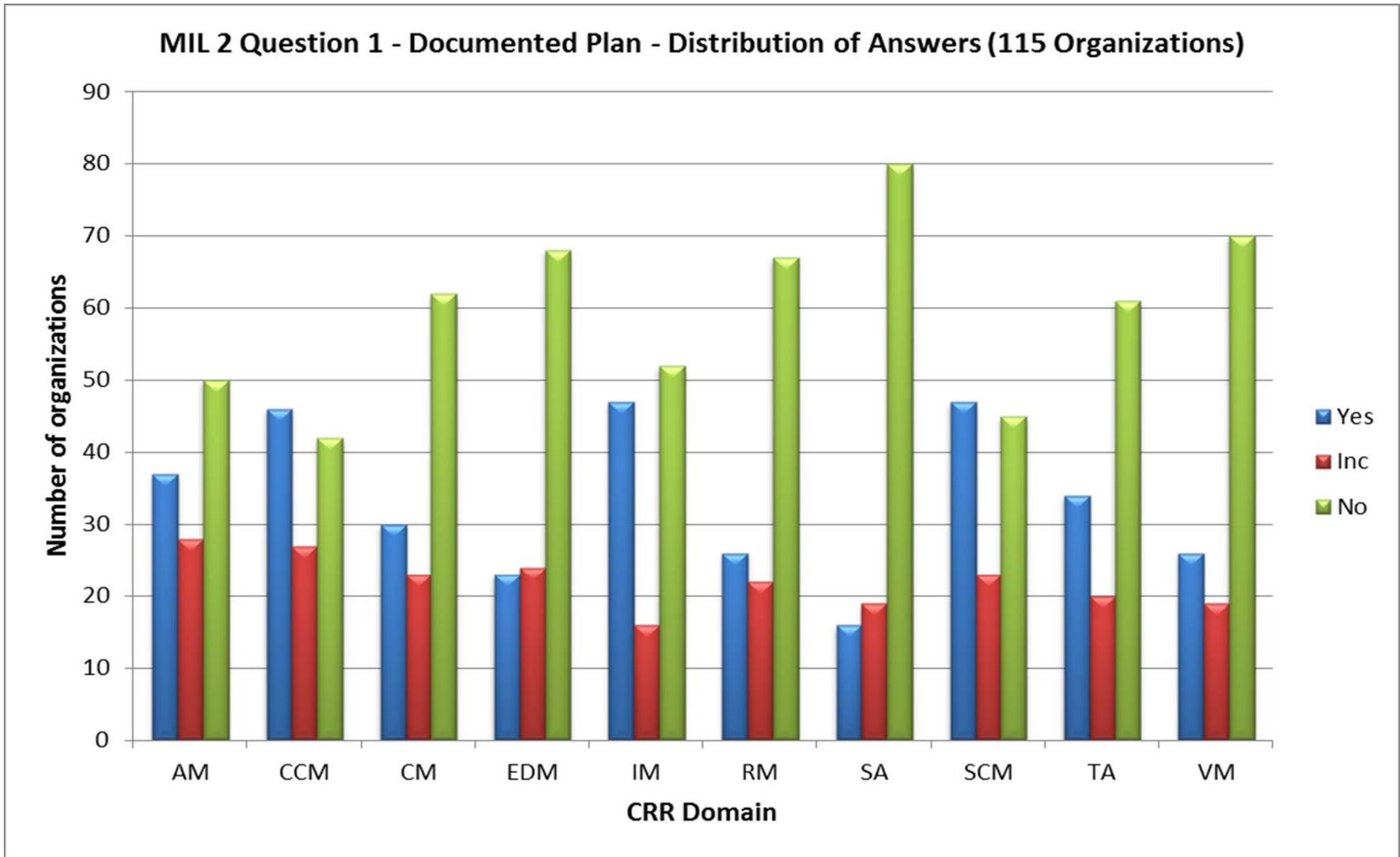


**Homeland
Security**

DHS CRR Analytical Findings – Cont.

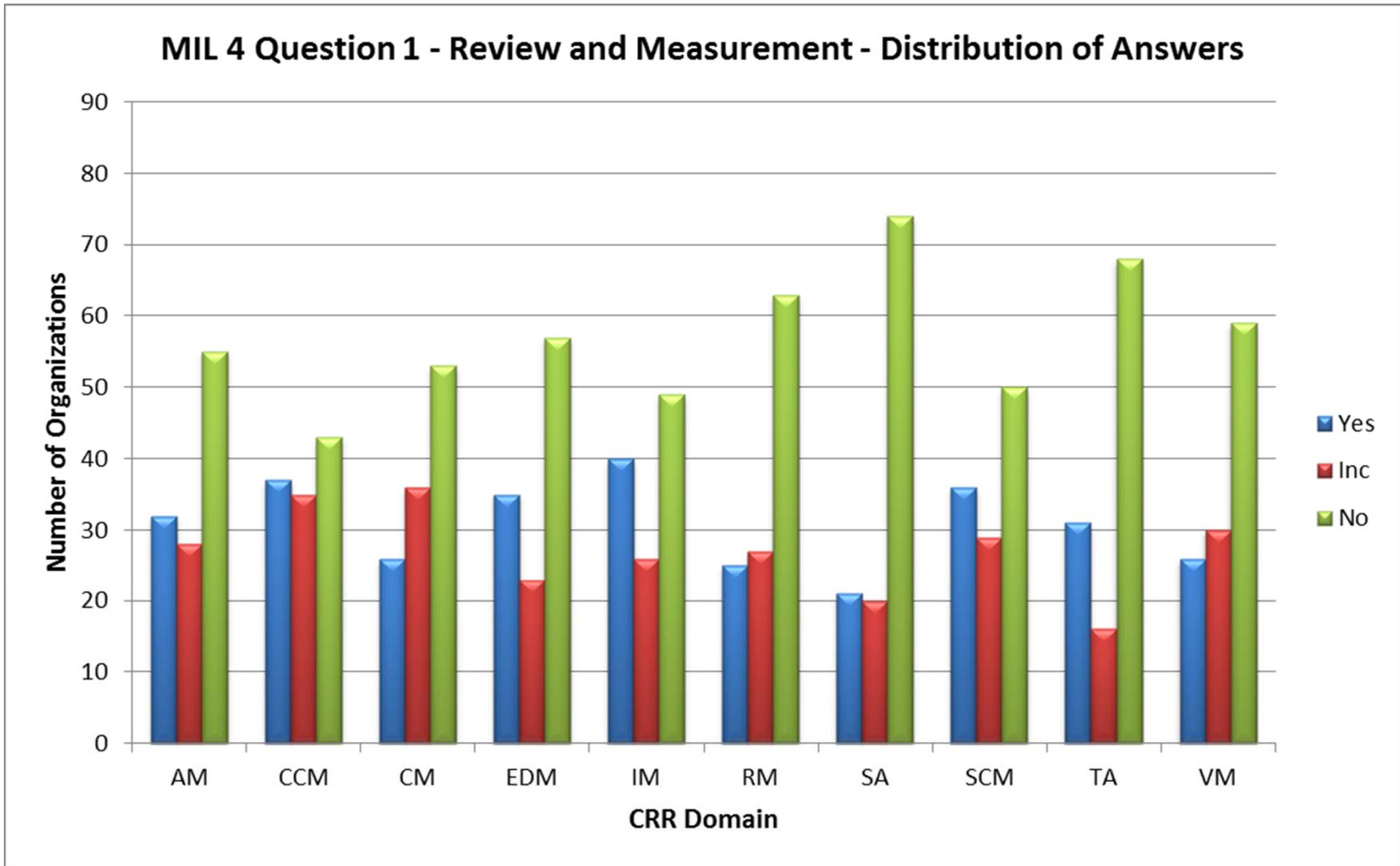


DHS CRR Analytical Findings – Cont.



Homeland Security

DHS CRR Analytical Findings – Cont.



Homeland Security

When Resilience Fails - NE Power Outage - August 14, 2003

Key Resilience Domains

AM	Asset Management <i>identify, document, and manage assets during their life cycle</i> 	IM	Incident Management <i>identify and analyze IT events, detect cybersecurity incidents, and determine an organizational response</i> 
CCM	Configuration and Change Management <i>ensure the integrity of IT systems and networks</i>	SCM	Service Continuity Management <i>ensure the continuity of essential IT operations if a disruption occurs</i> 
RISK	Risk Management <i>identify, analyze, and mitigate risks to critical service and IT assets</i> 	EXD	External Dependencies Management <i>establish processes to manage an appropriate level of IT, security, contractual, and organizational controls that are dependent on the actions of external entities</i> 
CNTL	Controls Management <i>identify, analyze, and manage IT and security controls</i> 	TRNG	Training and Awareness <i>promote awareness and develop skills and knowledge of people</i> 
VM	Vulnerability Management <i>identify, analyze, and manage vulnerabilities</i> 	SA	Situational Awareness <i>actively discover and analyze information related to immediate operational stability and security</i> 



DHS Cyber Resources – Operations Focused

- **National Cybersecurity and Communications Integration Center (NCCIC)**
 - Serves as a national center for reporting and mitigating communications and cybersecurity incidents.
<http://www.dhs.gov/about-national-cybersecurity-communications-integration-center>
 - Provides:
 - 24x7 real-time threat analysis and incident reporting capabilities, at 1-888-282-0870
 - Malware Submission Process:
 - Please send all submissions to: submit@malware.us-cert.gov
 - Must be provided in password-protected zip files using password “infected”
 - Web-submission: <https://malware.us-cert.gov>
 - ICS-CERT Training: <http://ics-cert.us-cert.gov/cscalendar.html>
- **Cyber Security Evaluations Program (cse@hq.dhs.gov)**
 - Provides no-cost, voluntary cyber security evaluations and assessments, including:
 - Cyber Resilience Review (CRR)
 - One-day, facilitated evaluation focused on critical IT services and the security management process
 - Cyber Security Evaluation Tool (CSET)
 - Stand-alone software application, used as a self-assessment against recognized standards and a tool for creating a baseline of cybersecurity practices
 - Downloadable at: http://us-cert.gov/control_systems/csetdownload.html



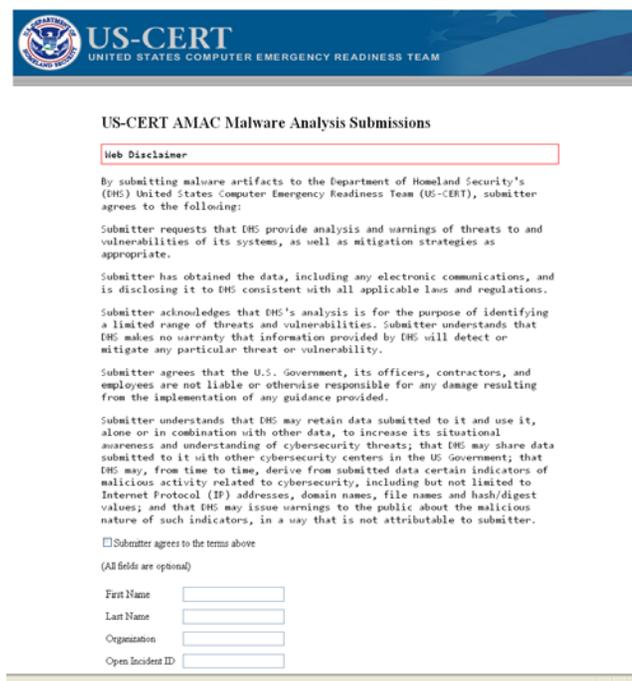
Additional - Incident Reporting

NCCIC provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870

Malware Submission Process:

- Please send all submissions to AMAC at:
submit@malware.us-cert.gov
- Must be provided in password-protected zip files using password “infected”
- Web-submission:
<https://malware.us-cert.gov>



The screenshot shows the top of a web page for US-CERT. The header includes the US-CERT logo and the text "US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM". Below the header is the title "US-CERT AMAC Malware Analysis Submissions". A red box highlights the "Web Disclaimer" section, which contains the following text:

By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following:

Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate.

Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations.

Submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability.

Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided.

Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter.

Submitter agrees to the terms above

(All fields are optional)

First Name

Last Name

Organization

Open Incident ID

FOUO / UNCLASS



Contact Information

Evaluation Inquiries

cse@hq.dhs.gov

General Inquiries

cyberadvisor@hq.dhs.gov

DHS Contact Information

Bradford Wilke
Program Manager, Cyber Security
Advisor Program

bradford.wilke@hq.dhs.gov
+1 412 375-4069

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications