Cybersecurity Advisor Program

To provide direct coordination, outreach, and regional support and assistance in the protection of cyber components essential to the Nation's Critical Infrastructure.

Sampling of CISA Offerings

- **Preparedness Activities**
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices
  - Cybersecurity Evaluations
    - Cyber Resilience Reviews (CRR™)
    - External Dependency Management Reviews
    - Cyber Infrastructure Surveys
    - Phishing Campaign Assessment
    - Vulnerability Scanning
    - Risk and Vulnerability Assessments (aka “Pen” Tests)
    - Cyber Security Evaluation Tool (CSET™)
    - Validated Architecture Design Review (VADR)

- **Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination

- **Cybersecurity Advisors**
  - Assessments
  - Working group collaboration
  - Best Practices private-public
  - Incident assistance coordination

- **Protective Security Advisors**
  - Assessments
  - Incident liaisons between government and private sector
  - Support for National Special Security Events

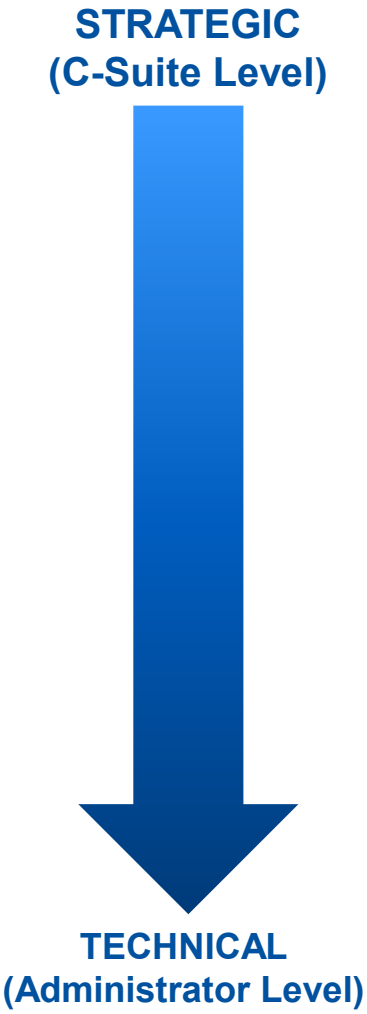
Range of Cybersecurity Assessments

Regional Resources:

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)

National Resources:

- Tabletop Exercises (Strategic/Technical)
- Phishing Campaign Assessment (Technical)
- Vulnerability Scanning / Hygiene (Technical)
- Web Applications Scanning (Technical)
- Validated Architecture Design Review (Technical)
- Risk and Vulnerability Assessment (Technical)

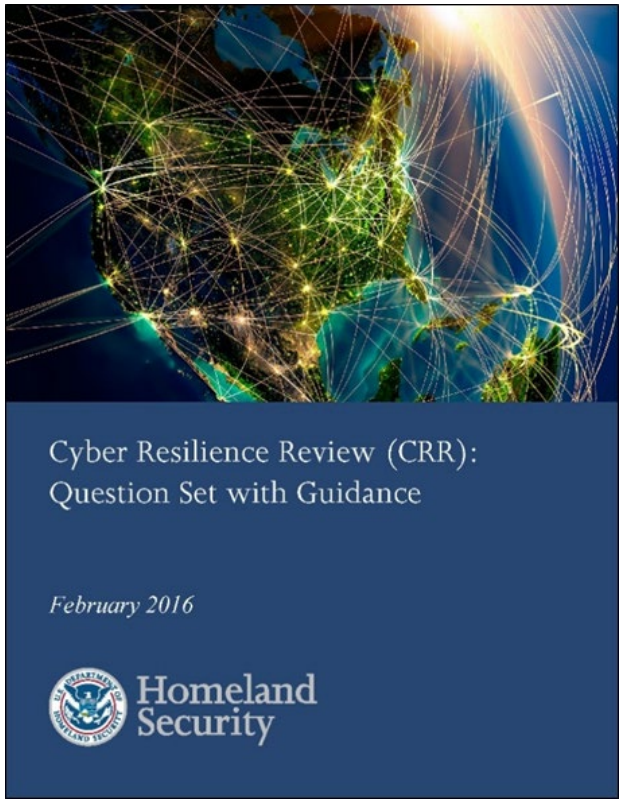


Cyber Resilience Review (CRR)

Purpose: The CRR is an assessment intended to evaluate an organization's operational resilience and cybersecurity practices of its critical services

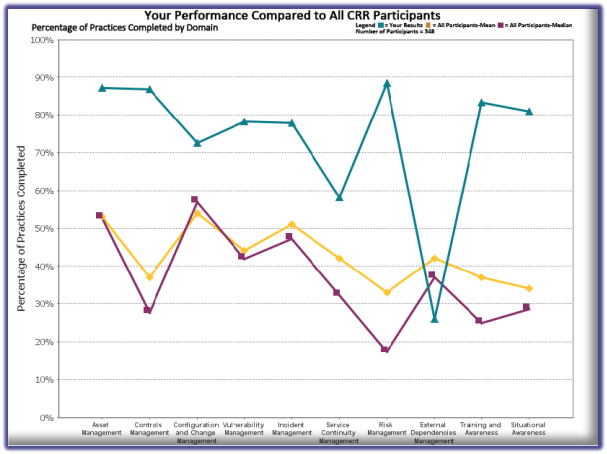
Delivery: The CRR can be

- Facilitated
- Self-administered
  - Cyber Resource Hub
  - https://www.cisa.gov/cyber-resource-hub



- Helps public and private sector partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk
- Based on the CERT ® Resilience Management Model (CERT® RMM)

Benefits of CRR

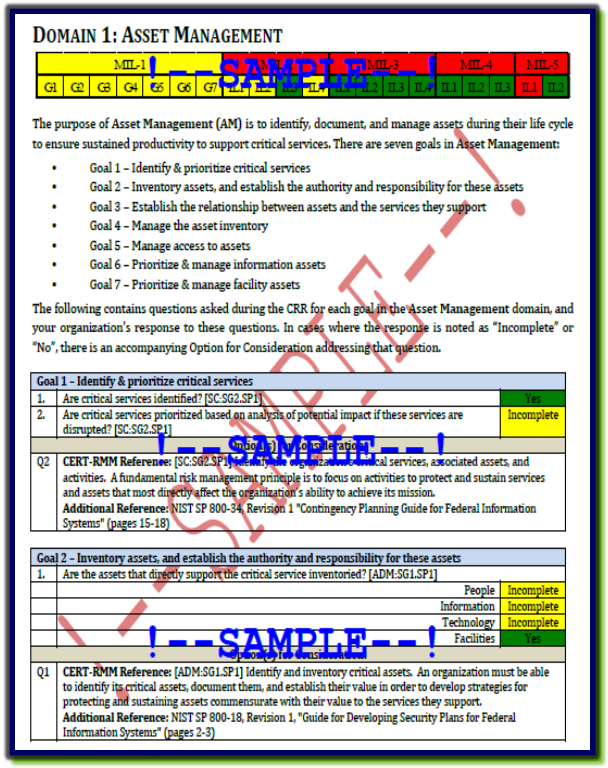


Comparison data with other CRR participants

**facilitated only*

A summary "snapshot" graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



CRR Mappings to Other Frameworks

The Cyber Resilience Review has been mapped to:

- NIST Cybersecurity Framework (CSF)
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT)
- NIST Special Pub 800-53 rev 4 (This mapping has not yet been published)

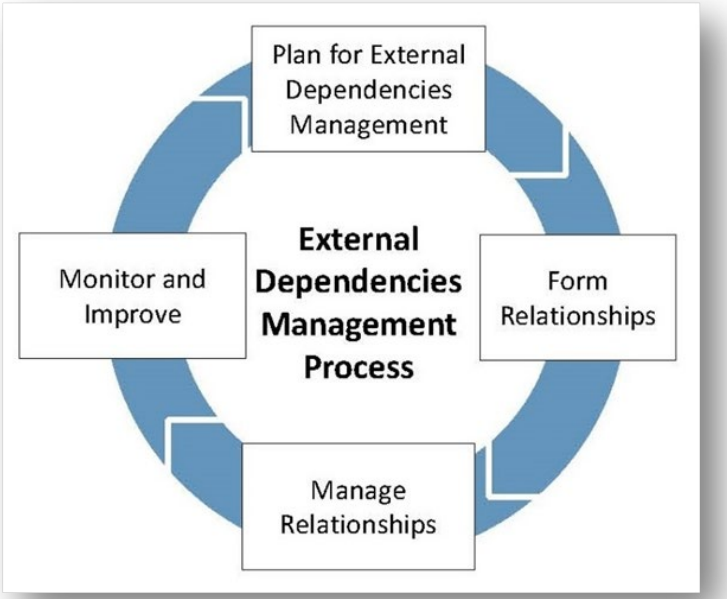
Most Cybersecurity Frameworks are being mapped to the NIST Cybersecurity Framework as a result that mapping can be used to indirectly map them to the CRR

External Dependency Management (EDM)

Overview: In 2016, DHS launched the External Dependencies Management (EDM) Assessment, focusing specifically on ensuring the protection and sustainment of services and assets that are dependent on the actions of third-party entities.

Background: External Dependencies Management is a domain covered by the CRR. However, EDM and associated issues (e.g., supply-chain management, vendor management) are not addressed at a comprehensive level within the CRR, resulting in the creation of a separate assessment.

Linkages to CRR: Despite operating at a more granular level than the CRR, the EDM Assessment borrows heavily from the CRR's methodological architecture and scoring system but remains a DHS-facilitated assessment.



EDM process outlined in the External Dependencies Management Resource Guide

External Dependency Management (EDM)

To provide the organization with an understandable and useful structure for the evaluation, the EDM Assessment is divided into three distinct areas (domains):

1. **RELATIONSHIP FORMATION** – how the organization considers third party risks, selects external entities, and forms relationships with them so that risk is managed from the start
2. **RELATIONSHIP MANAGEMENT AND GOVERNANCE** – how the organization manages ongoing relationships with external entities to support and strengthen its critical services at a managed level of risk and cost
3. **SERVICE PROTECTION AND SUSTAINMENT** – how the organization plans for, anticipates, and manages disruption or incidents related to external entities

Cybersecurity Infrastructure Survey (CIS)

Structured, interview based assessment (2 ½ to 4 hours) of essential cybersecurity practices in-place for critical services within your organization

Identifies interdependencies, capabilities, and the emerging effects related to current cybersecurity posture

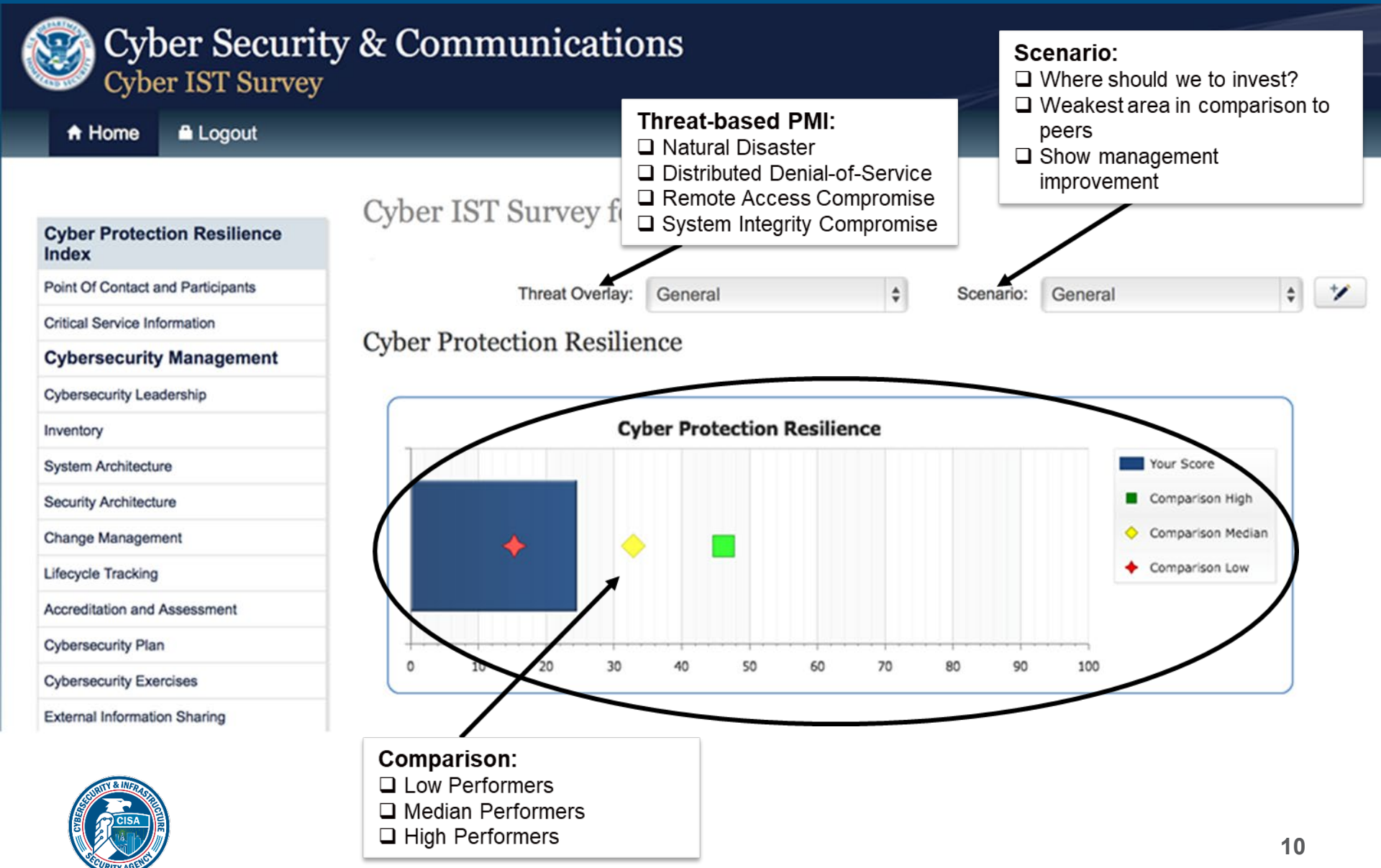
Focuses on protective measures, threat scenarios, and a service based view of cybersecurity in context of the surveyed topics

Broadly aligns to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

CIS Survey Question Domains

CIS Domains	
Cybersecurity Forces	**Cybersecurity Management**
* Personnel	* Cybersecurity Leadership
* Cybersecurity Training	* Cyber Service Architecture
Cybersecurity Controls	* Change Management
* Authentication and Authorization Controls	* Lifecycle Tracking
* Access Controls	* Assessment and Evaluation
* Cybersecurity Measures	* Cybersecurity Plan
* Information Protection	* Cybersecurity Exercises
* User Training	* Information Sharing
* Defense Sophistication and Compensating Controls	**Dependencies**
Incident Response	* Data at Rest
* Incident Response Measures	* Data in Motion
* Alternate Site and Disaster Recovery	* Data in Process
	* End Point Systems

Example CIS Dashboard



National Resources

Cyber Exercise & Planning Program

CISA designs, develops, conducts, and evaluates cyber exercises ranging from small-scale, limited scope, discussion-based exercises to large-scale, internationally-scoped, operations-based exercises.

CISA offers the following services at no-cost on an as-needed and as-available basis:

- Cyber Storm Exercise (CISA's flagship national level cyber exercise)
- End-to-End Cyber Exercise Planning
- Cyber Exercise Consulting
- Cyber Planning Support
- Exercise-In-A-Box
- Virtual CTTX

Phishing Campaign Assessment (PCA)

Objectives:

- Increase cybersecurity awareness within stakeholder organizations
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation

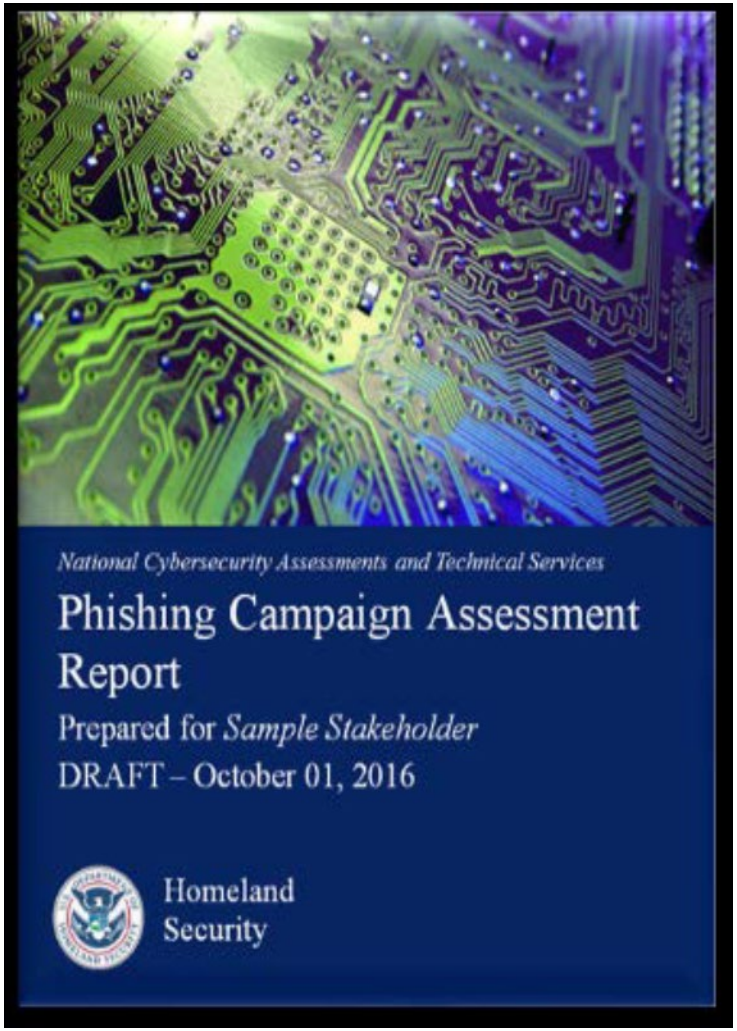
Benefits:

- Receive actionable metrics
- Highlight need for improved security Training

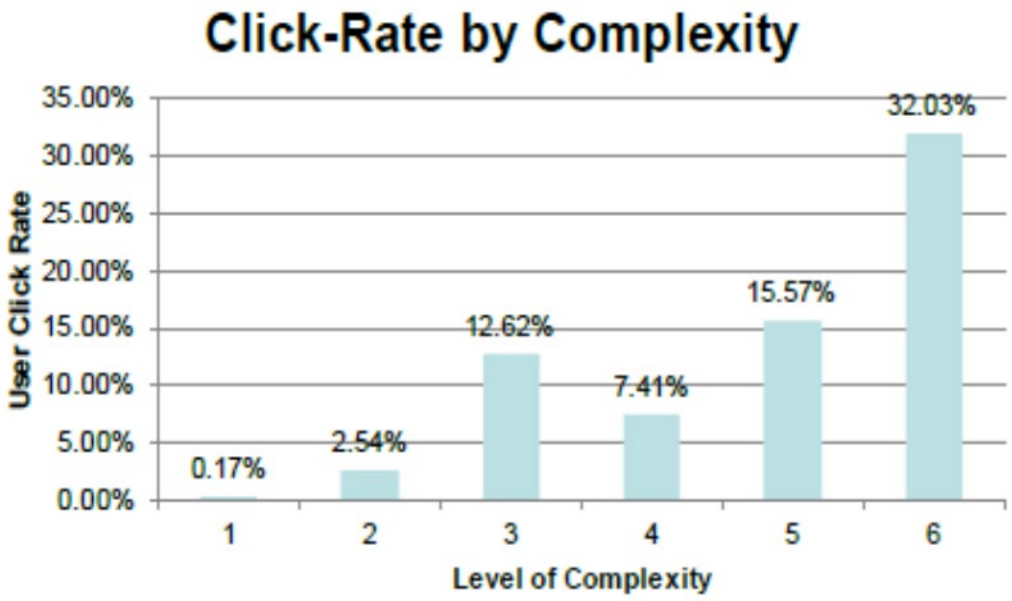
Scope:

- 6-week engagement period
- Phishing emails capture click-rate only, no payloads will be used
- Varying Levels of Complexity -- Levels 1 - 6 (Easy to Difficult)

Phishing Campaign Assessment (PCA)



Week	Campaign	Date Sent	Complexity Level	User Click Rate	# Emails Sent
1	Please Help!	3/18/16	1	0.17%	401
2	Reveal Your Past	3/31/16	2	2.54%	402
3	Password Expire Alert	4/6/16	3	12.62%	401
4	Severe Weather Checklist	4/15/16	4	7.41%	402
5	Federal Employee Survey	4/20/16	5	15.57%	401
6	Salary Guidelines	4/27/16	6	32.03%	402



Vulnerability Scanning Service (CyHy)

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

Web Application Scanning (WAS)

An Internet based scanning service to assess the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.

SCANNING OBJECTIVES

- Maintain enterprise awareness of your publicly accessible web-based assets
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities to help reduce overall risk

SCANNING PHASES

- Discovery Scanning: Identify active, internet-facing web applications
- Vulnerability Scanning: Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

Remote Penetration Test (RPT)

Utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.

- Focuses on externally accessible systems

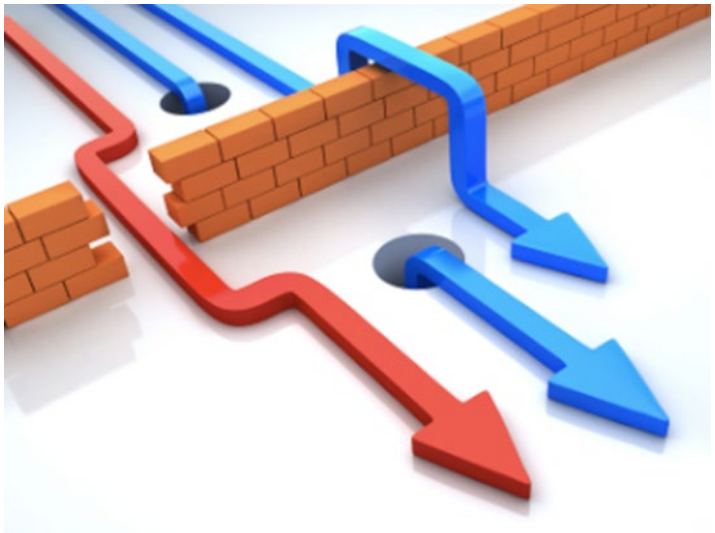
SCENARIOS:

- **External Penetration Test**: Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.
- **External Web Application Test**: Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.
- **Phishing Assessment**: Testing through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.

Risk and Vulnerability Assessment (RVA)

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

- 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



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.

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

Hunt & Incident Response Team (HIRT)

Incident Triage: Process taken to scope the severity of an incident and determine required resources for action

Network Topology Review: Assessment of network ingress, egress, remote access, segmentation, and interconnectivity, with resulting recommendations for security enhancements

Infrastructure Configuration Review: Analysis of core devices on the network which are or can be used for network security (e.g., prevention, monitoring, or enforcement functions)

Log Analysis: Examination of logs from network and security devices to illuminate possible malicious activity

Incident Specific Risk Overview: Materials and in-person briefings for technical, program manager, or senior leadership audience; cover current cyber risk landscape, including classified briefings to cleared staff when appropriate

Hunt Analysis: Deployment of network hunting tools to proactively detect indicators of compromise (IOC)

Security Program Review: A review of the client's existing security roles, responsibilities, and policies to identify possible organizational or information-sharing gaps

Malware Analysis: Reverse engineering of malware artifacts to determine functionality and build indicators

Mitigation: Actionable guidance to improve the organization's security posture, including incident-specific recommendations, security best practices, and recommended tactical measures

Digital Media Analysis: Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators

Control Systems Incident Analysis: Analysis of supervisory control and data acquisition devices, process control, distributed control, and any other systems that control, monitor, and manage critical infrastructure

Additional Cyber Resources

CISA Website (www.CISA.gov)

CISA Cyber Essentials
https://www.cisa.gov/publication/cisa-cyber-essentials

CISA Ransomware Resources
https://www.cisa.gov/stopransomware

Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CISA Shields Up
https://www.cisa.gov/shields-up

Maintain Situational Awareness

National Council of ISAC's

Information Sharing and Analysis Centers (ISACs) help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency

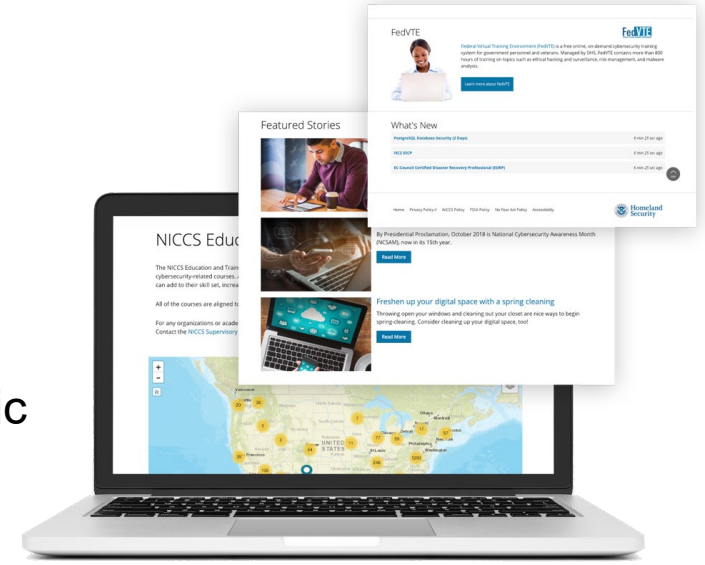
https://www.nationalisacs.org/member-isacs-3

Cybersecurity Training Resources

CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Searchable Training Catalog with 4,400 plus cyber-related courses offered by nationwide cybersecurity educators
- Interactive National Cybersecurity Workforce Framework
- Cybersecurity Program information: FedVTE, Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and resources for cyber managers
- Upcoming cybersecurity events list



For more information: https://niccs.us-cert.gov/training/search

Federal Virtual Training Environment (FedVTE)

Cyber professionals can continue to improve their skills through hands-on training opportunities.

FedVTE is an online, on-demand training center that provides free cybersecurity training for federal, state, local, tribal, and territorial government employees and to U.S. veterans.

FedVTE offers a limited number of courses to the public. Public course user progress and completions are not tracked or stored by the FedVTE system.

https://fedvte.usalearning.gov

IMR Training Series

The Identify, Mitigate, and Recover (IMR) incident response curriculum provides a range of training offerings encompassing cybersecurity awareness and best practices for organizations, live red/blue team network defense demonstrations emulating real-time incident response scenarios, and hands-on cyber range training courses for incident response practitioners.

Topics for Awareness Webinars & Cyber Range Training:

- Ransomware
- Cloud Security
- Business Email Compromise
- Vulnerabilities of Internet-Accessible Systems
- Web and Email Server Attacks
- DNS Infrastructure Attacks
- High Value Assets/Critical Assets
- Indicators of Compromise
- Incident Analysis with tool demo
- Investigating logs for incidents

Topics for Cyber Range Challenges & Observe the Attack Series:

- Ransomware
- Cloud Security
- Business Email Compromise

For more info: education@cisa.dhs.gov
Or visit: https://www.cisa.gov/incident-response-training

CISA Incident Reporting

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities.

Where to report:

https://www.cisa.gov/uscert/report

24x7 contact number: 888-282-0870

Email: Report@cisa.gov

John E. Busch
Protective Security Advisor
Region 5 – Wisconsin District
Phone: 414-369-8540
Email: john.busch@hq.dhs.gov

David Melby
Protective Security Advisor
Region 5 – Wisconsin District
Phone: 608-405-2931
E-mail: david.melby@cisa.dhs.gov

Bill Nash
Cybersecurity Advisor
Region 5 – Wisconsin District
Phone: 608-590-7105
Email: william.nash@cisa.dhs.gov