NEW YORK STATE | Homeland Security and Emergency Services

DHSES Cyber Incident Response Team (CIRT)

Safeguarding County Systems, Services, and Infrastructure

March 24, 2022

Mission Objectives

Identify / Prevent / Protect

- Risk and Vulnerability Assessments
- Training and Exercises
- Information Sharing and Outreach

Respond / Recover

- Incident response and digital forensics
- Remediation assistance

Threat Briefing

2022 Russia-Ukaine Cyber Activity

- Primary activity
  - DDoS Attacks
  - Targeted Phishing
  - Wiper Malware
  - Disinformation campaign
  - Non associated groups supporting both efforts
  - Global scanning activity – uptick in US targeted scanning from Russia
- CISA and FBI report - no specific, credible threat to the U.S. homeland at this time
- While Russia is already engaged in cyber-attacks aimed at Ukraine, the FBI and DHS are concerned about potential cyberattacks or spillover to organizations within the United States
- https://www.cisa.gov/shields-up

NEW YORK STATE | Homeland Security and Emergency Services

Threat Briefing

2020/2021 challenges and opportunities

- Supply chain and zero-day attacks

Vulnerabilities being exploited by cyber criminals and nation state actors

  - Citrix Netscaler - CVE-2019-19781
  - Netlogin - CVE-2020-1472
  - Solarwinds Supply Chain Attack
  - Pulse Secure
  - Exchange
  - Log4j

- Data Exfiltration in Conjunction with Ransomware
- Health Care facilities being targeted during COVID outbreak
- Phishing, Smishing combined fake site landing pages (DMV,DOL)
- Web Defacements
- DDoS Attacks

CIRT Observations

2020/2021 challenges and opportunities

- No MFA – VPN, RDP, Email, HR/Payroll Systems
- No logging or not properly configured / reviewed
- AV Alerts not followed up on
  - Partial cleaning, infection persists
- Segmentation, identify critical system
- Mitigations, patching, verification
- RDP Exposed directly to the internet?

Recommendations

Implement a defense in depth strategy

- Backup critical systems and data and keep offline copies (3-2-1 backup)
- Keep all systems up-to-date (Patch)- (remove EOL equipment)
- Ensure proper logging and alerting is in place
- Investigate all alerts/events (even if they were reported to be clean/blocked)
- Implement email filtering
- Use multifactor authentication
- Provide cyber awareness training to end users
- Practice least privilege
  - Disable file sharing where unnecessary
  - Limit access for script and macro and execution
  - Segment your networks with firewalls and ACLs
- Review and exercise your Cyber Incident Response Plan

Before a Cyber Incident

- Develop and test your incident response plans
  - Don’t just document an IR plan, perform a tabletop or dry run to make sure all processes work as expected

- Document key stakeholders that need to be involved (executive leadership, legal, cyber insurance)

- Know who to contact and when to escalate

During a Cyber Incident

What to think about

- Rely on your plan
- Determine the scope of what happened
    - Disable network access and preserve digital artifacts
- Contain, understand and remove the threat *before* you recover
- Communicate internally and externally with stakeholders
    - Contact state law enforcement, FBI, CISA, DHSES – 1-844-OCT-CIRT
    - Work with your managed service providers and vendors

- Don’t forget to learn from what happened!

Prepare

DR/BC

Controlled Administrative Access and Account Control

Secure Configurations

Inventory Of Hardware and Software

Vulnerability Management

Multi Factor Authentication

Inventory and Data Classification

Cyber Security Framework Adoption and Program Development

Malware Defenses

Boundary Defense

Maintenance, Monitoring, Logging

Security Awareness Training

Cyber and Enterprise Risk Assessments

Incident Response Plans

Patch Management

Vendor Risk Management

NEW YORK STATE | Homeland Security and Emergency Services

Proactive Services

Before a Cyber Incident Occurs

How DHSES CIRT can assist:

- Cybersecurity Risk Assessments (CIS Controls v8)
  - PCII protected report
  - Prioritized list of risks
  - We focus on low/no cost solutions
- Phishing Exercises
- Tabletop Exercises
- Cybersecurity Grant Program

All DHSES CIRT services are provided at <u>no cost</u> to non-executive agencies, local governments and public authorities

NEW YORK STATE | Homeland Security and Emergency Services

Cybersecurity Risk Assessments

Cybersecurity Risk Assessment

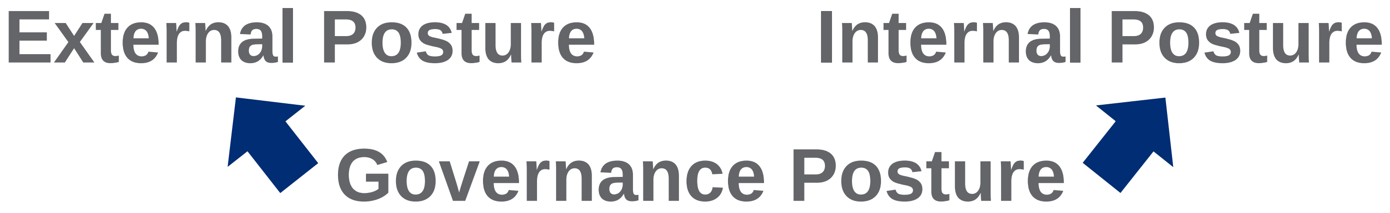
How DHSES CIRT can assist:

- Edge Assessment Service
- Onsite Vulnerability Scanning
- Posture Assessment

- We provide a written report identifying potential weaknesses and assistance afterwards remediating those weaknesses

- These are provided jointly with National Guard team members

Cybersecurity Risk Assessment Pillars

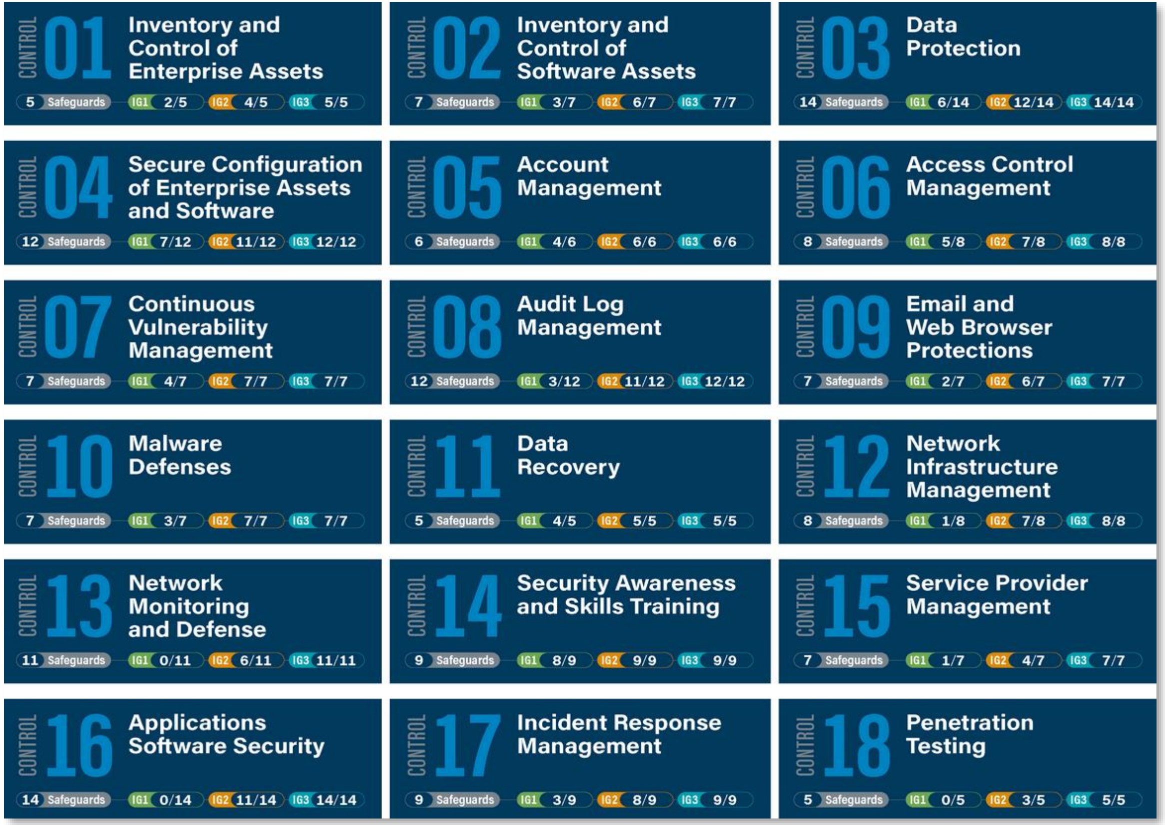


External Posture

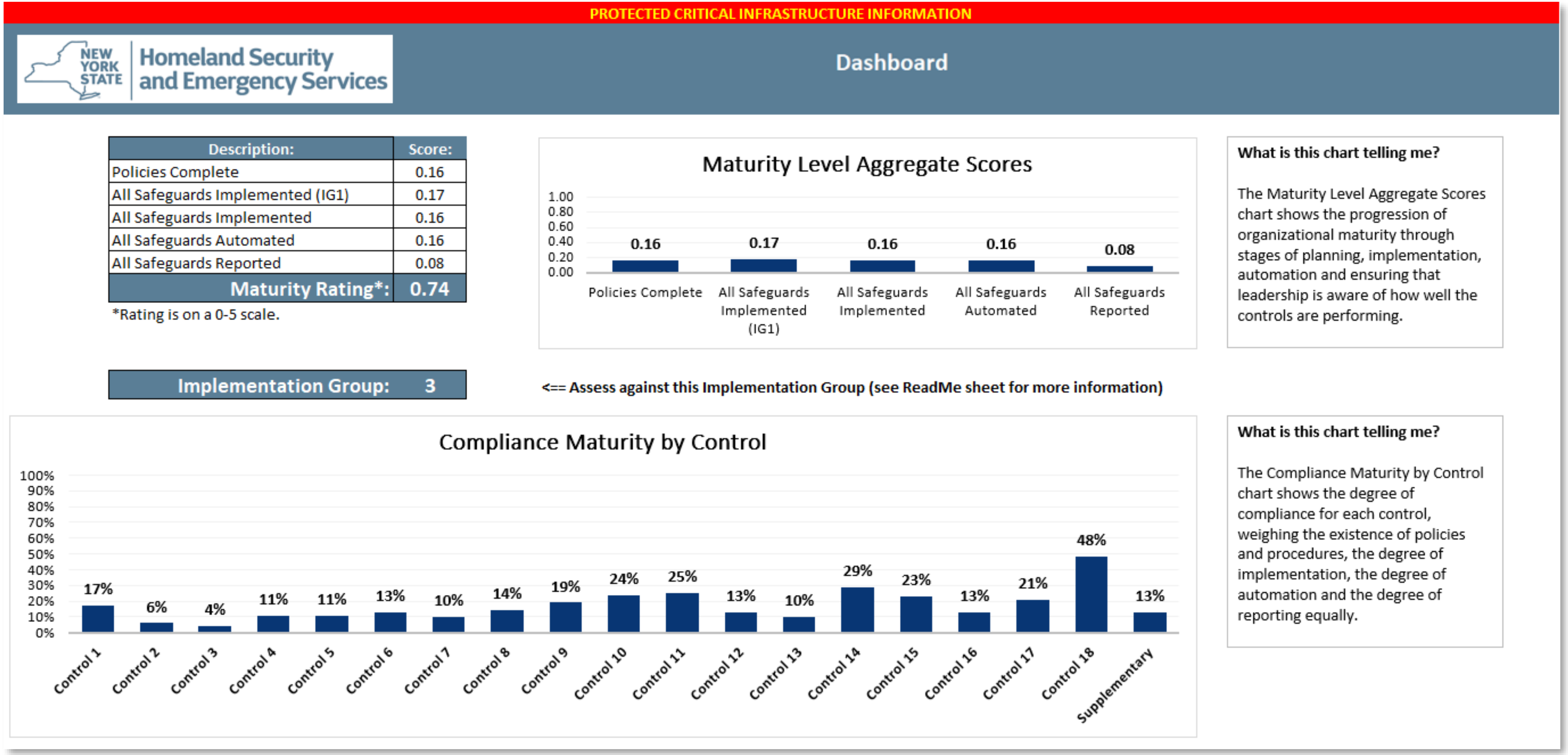
Internal Posture

Governance Posture

CIS Controls



CONTROL		Safeguards	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets	5	2/5	4/5	5/5
02	Inventory and Control of Software Assets	7	3/7	6/7	7/7
03	Data Protection	14	6/14	12/14	14/14
04	Secure Configuration of Enterprise Assets and Software	12	7/12	11/12	12/12
05	Account Management	6	4/6	6/6	6/6
06	Access Control Management	8	5/8	7/8	8/8
07	Continuous Vulnerability Management	7	4/7	7/7	7/7
08	Audit Log Management	12	3/12	11/12	12/12
09	Email and Web Browser Protections	7	2/7	6/7	7/7
10	Malware Defenses	7	3/7	7/7	7/7
11	Data Recovery	5	4/5	5/5	5/5
12	Network Infrastructure Management	8	1/8	7/8	8/8
13	Network Monitoring and Defense	11	0/11	6/11	11/11
14	Security Awareness and Skills Training	9	8/9	9/9	9/9
15	Service Provider Management	7	1/7	4/7	7/7
16	Applications Software Security	14	0/14	11/14	14/14
17	Incident Response Management	9	3/9	8/9	9/9
18	Penetration Testing	5	0/5	3/5	5/5



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

NEW YORK STATE Homeland Security and Emergency Services

Dashboard

Description:	Score:
Policies Complete	0.16
All Safeguards Implemented (IG1)	0.17
All Safeguards Implemented	0.16
All Safeguards Automated	0.16
All Safeguards Reported	0.08
Maturity Rating*:	0.74

*Rating is on a 0-5 scale.

What is this chart telling me?

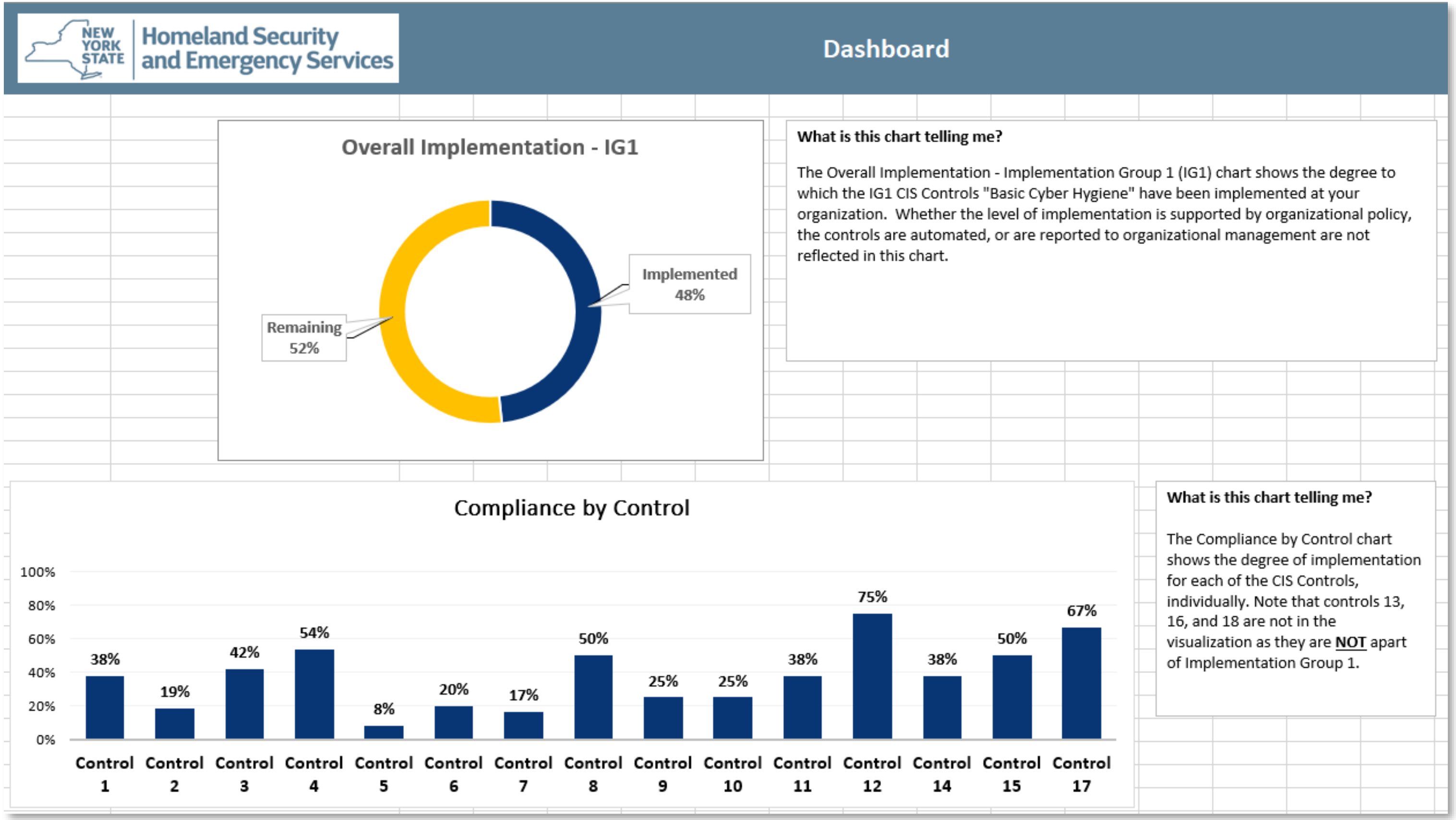
The Maturity Level Aggregate Scores chart shows the progression of organizational maturity through stages of planning, implementation, automation and ensuring that leadership is aware of how well the controls are performing.

Implementation Group: 3

<== Assess against this Implementation Group (see ReadMe sheet for more information)

What is this chart telling me?

The Compliance Maturity by Control chart shows the degree of compliance for each control, weighing the existence of policies and procedures, the degree of implementation, the degree of automation and the degree of reporting equally.



Dashboard

What is this chart telling me?

The Overall Implementation - Implementation Group 1 (IG1) chart shows the degree to which the IG1 CIS Controls "Basic Cyber Hygiene" have been implemented at your organization. Whether the level of implementation is supported by organizational policy, the controls are automated, or are reported to organizational management are not reflected in this chart.

What is this chart telling me?

The Compliance by Control chart shows the degree of implementation for each of the CIS Controls, individually. Note that controls 13, 16, and 18 are not in the visualization as they are <u>NOT</u> apart of Implementation Group 1.

Phishing Exercises and Awareness

Phishing Exercises and Awareness

- DHSES CIRT works with you to craft a phishing test that’s appropriate to your organizational mission and current cyber-maturity

- Information about how your users interact with the phishing messages is tracked along with any training progress

- After testing, our team provides a report that can be leveraged to jump start your cyber security awareness training efforts and help minimize risk

Cyber Tabletop Exercises

Cyber Tabletop Exercises

- These exercises help organizations understand how well its IR plans work during a cybersecurity incident
- The DHSES CIRT facilitates an exercise built around a scenario tailored specifically to your organization and its plans
- The exercise includes key stake holders from within the organization:
  - IT Director/Staff
  - Legal
  - Executive Staff
  - PIO
  - Law Enforcement

Reactive Services

Incident Response, Forensics, and Analysis

How DHSES CIRT can assist:

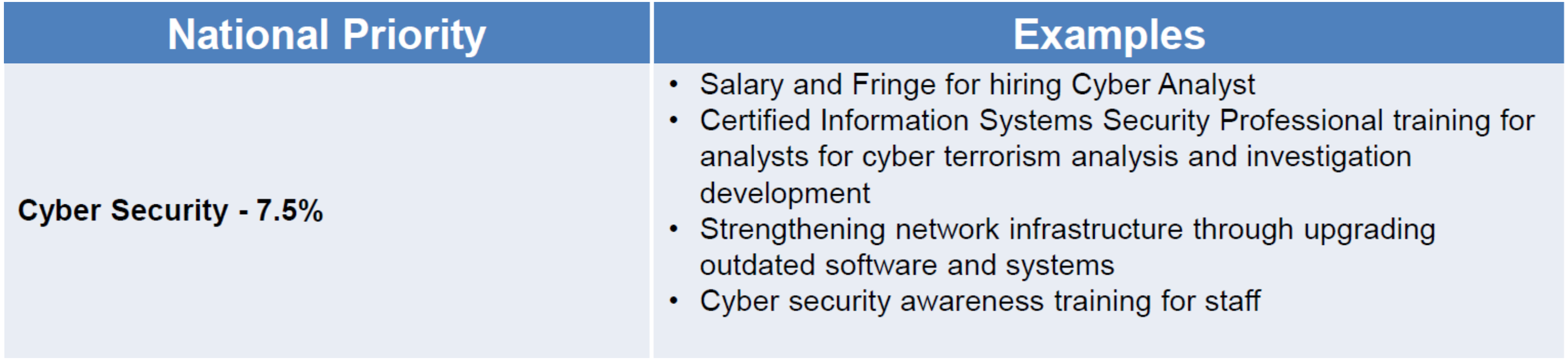
- Incident Response and Recovery Guidance
- Digital Forensics
- Log, Malware and Root Cause analysis
  - It is critical to identify how a cyber intrusion happened to prevent re-occurrence

All DHSES CIRT services are provided at no cost to non-executive agencies, local governments and public authorities

Cybersecurity Grant Program

Cybersecurity Grant Program

- Supports enhancement and sustainment of cyber security capabilities for local governments by ensuring their information systems are protected from cyber incidents
- 7.5% of all SHSP and UASI grants funds must be devoted to cybersecurity projects



National Priority	Examples
Cyber Security - 7.5%	• Salary and Fringe for hiring Cyber Analyst • Certified Information Systems Security Professional training for analysts for cyber terrorism analysis and investigation development • Strengthening network infrastructure through upgrading outdated software and systems • Cyber security awareness training for staff

Cybersecurity Project Planning

Common Cyber Projects

- Multi-Factor Authentication (MFA)
- Email / Spam Filters
- User Training
- Network Filtering (Firewalls – IDS/IPS)
- Patch Management Software
- Privilege Access Management
- Incident Response Planning
- Policy Development and Review
- Endpoint Protection, Detection & Response
- Application Allow Listing
- Network Segmentation
- Hardware and Software Inventory
- Data Classification
- Backup Solutions
- Cybersecurity Risk Assessment

Cyber Services Recap

Cyber Services Recap

Proactive Services

- Cybersecurity Risk Assessments
- Phishing / Training Exercises
- Cyber Tabletop Exercises

Reactive Services

- Incident Response Guidance
- Digital Forensics
- Log/Root Cause/Malware Analysis

Contact Information

Contact Information

Contact DHSES Cyber Incident Response Team (CIRT)

- To report a cyber incident, please call: 1 (844) OCT-CIRT | 1 (844) 628-2478
- To request DHSES CIRT cyber support, please email: CIRT@dhses.ny.gov
- For more information, please visit: https://www.dhses.ny.gov/cyber-incident-response-team

Questions?