2022 CHEMICAL SECURITY SUMMIT

August 23-25, 2022

#ChemicalSecurity

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

CHEMICAL SECURITY SUMMIT

Cybersecurity for Physical Security Professionals

Kelly Murray

Associate Director, CISA Chemical Security

Michael Morgan

Chief Information Security Officer, Phillips 66

Moderator: Jake Mehl

Section Chief, Chemical Sector Management Team, CISA

#ChemicalSecurity

Cybersecurity Stats

AKA: why you really SHOULD care about cyber…even if you're not a "cyber guy"

- Cyber systems are integrated throughout the operations of facilities that possess chemicals.
- A good cybersecurity posture takes a comprehensive view of all cyber systems and uses a layered approach of policies, practices, and people to prevent, protect against, respond to, and recover from cyber sabotage or incidents.

Quick Stats:

- In 2021, there was a ransomware attack every 11 seconds
- 43% of cyber-attacks target small businesses
- Supply chain cyber-attacks grew 420%
- The FBI estimates phishing attacks may increase by as much as 400% year-over-year
- 30% of phishing emails are opened
- The average cost of a data breach is $3.86M
- One company reported as many as 78% of emails received monthly are malicious

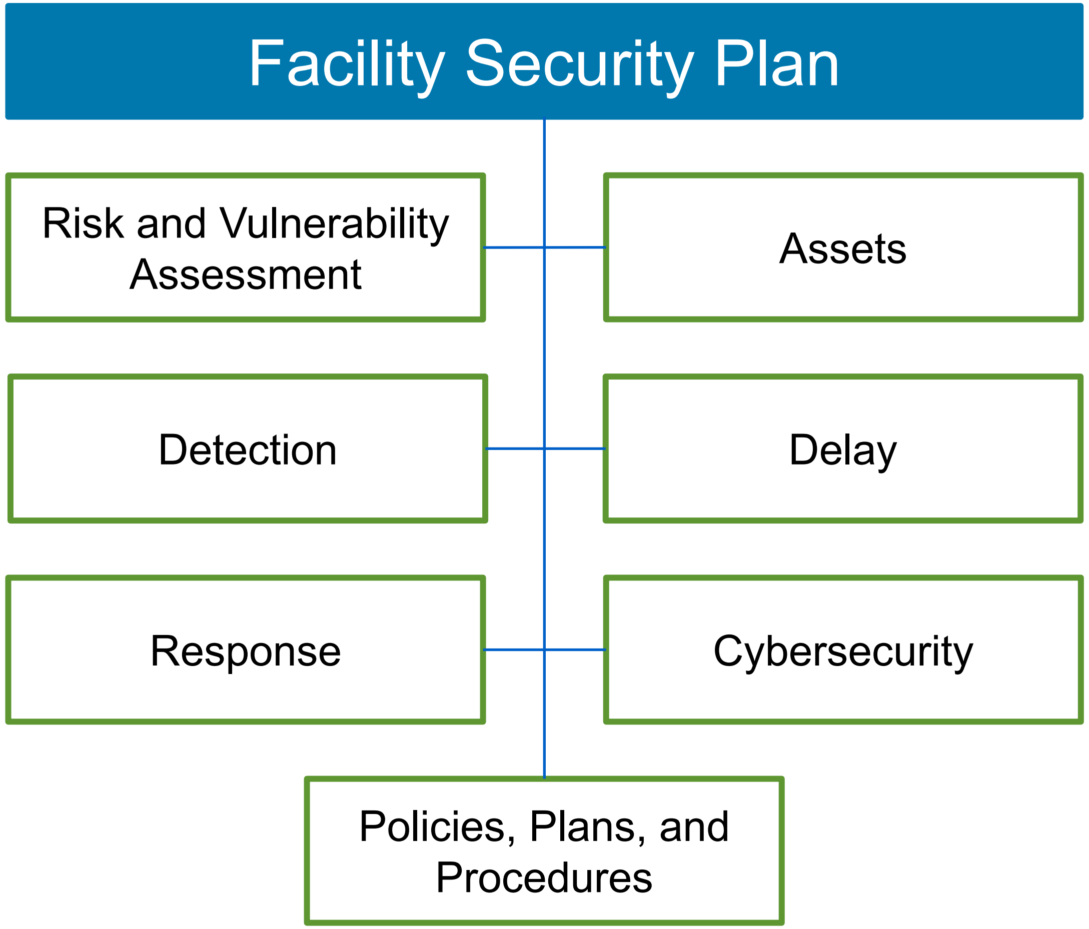
Types of Cyberattacks

- **Malware**: Harmful software distributed through a computer’s system (often requiring the user to take an action, such as clicking on an email attachment). Examples of malware include viruses, worms, malicious mobile code, Trojan horses, rootkits, spyware, and some forms of adware.
- **Ransomware**: A type of malware that encrypts data that can only be unlocked when ransom is paid.
- **Man-in-the-Middle Attack**: An interruption into a two-party transaction that allows attackers to filter and steal data during the transaction.
- **Pharming/ Watering Hole Attacks**: A means of directing users to a malicious or illegitimate website by redirecting the original uniform resource locator (URL) or an attack that involves corrupting a highly trafficked website, so that a user’s computer is also infected when visiting the corrupt website.
- **Phishing**: Fraudulent emails, text messages, or websites purporting to be from a trusted source that require action, such as sending money or confidential documents to the “source.”

Secure Your Chemicals

Cybersecurity is one part of a larger security plan

- A security plan serves as a management tool to guide a facility's security and response efforts.
- A strong security plan integrates all major security goals into a holistic approach.
- This reduces duplication of effort and allows facilities to identify security gaps.



Facility Security Plan
Risk and Vulnerability Assessment
Assets
Detection
Delay
Response
Cybersecurity
Policies, Plans, and Procedures

Cybersecurity Principles and Initiatives

Step 1: Identify Your Cyber Systems

Consider what systems could impact the security of the COI.

- Physical Security Systems
  - Access control or other electronic security that is connected to other systems
    - Does the facility employ an intrusion detection system or cameras?
- Business Systems
  - Inventory management systems
  - Ordering, shipping, and receiving systems
- Process and Control Systems
  - Systems that monitor or control physical processes that contain COI
    - Does the facility employ control systems (ICS, DCS, SCADA)?

Step 2: Cyber Vulnerability Assessment

Identify whether your critical cyber systems, networks, hardware, and software have vulnerabilities that could be exploited by an attacker.

Learn more or sign up at:

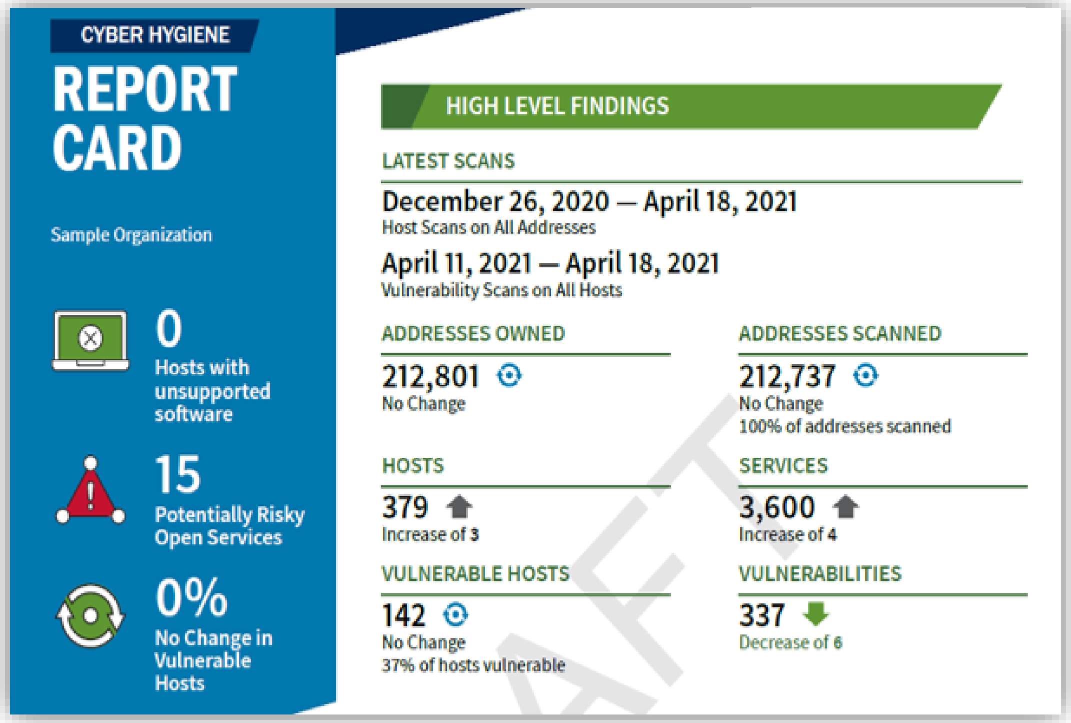
cisa.gov/cyber-assessments

cisa.gov/cyber-essentials

cisa.gov/cyber-hygiene-services

CYBER ESSENTIALS

Your success depends on *Cyber Readiness*. Both depend on *YOU*.



CYBER HYGIENE

REPORT CARD

Sample Organization

0 Hosts with unsupported software

15 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

December 26, 2020 — April 18, 2021
Host Scans on All Addresses

April 11, 2021 — April 18, 2021
Vulnerability Scans on All Hosts

ADDRESSES OWNED
212,801
No Change

ADDRESSES SCANNED
212,737
No Change
100% of addresses scanned

HOSTS
379
Increase of 3

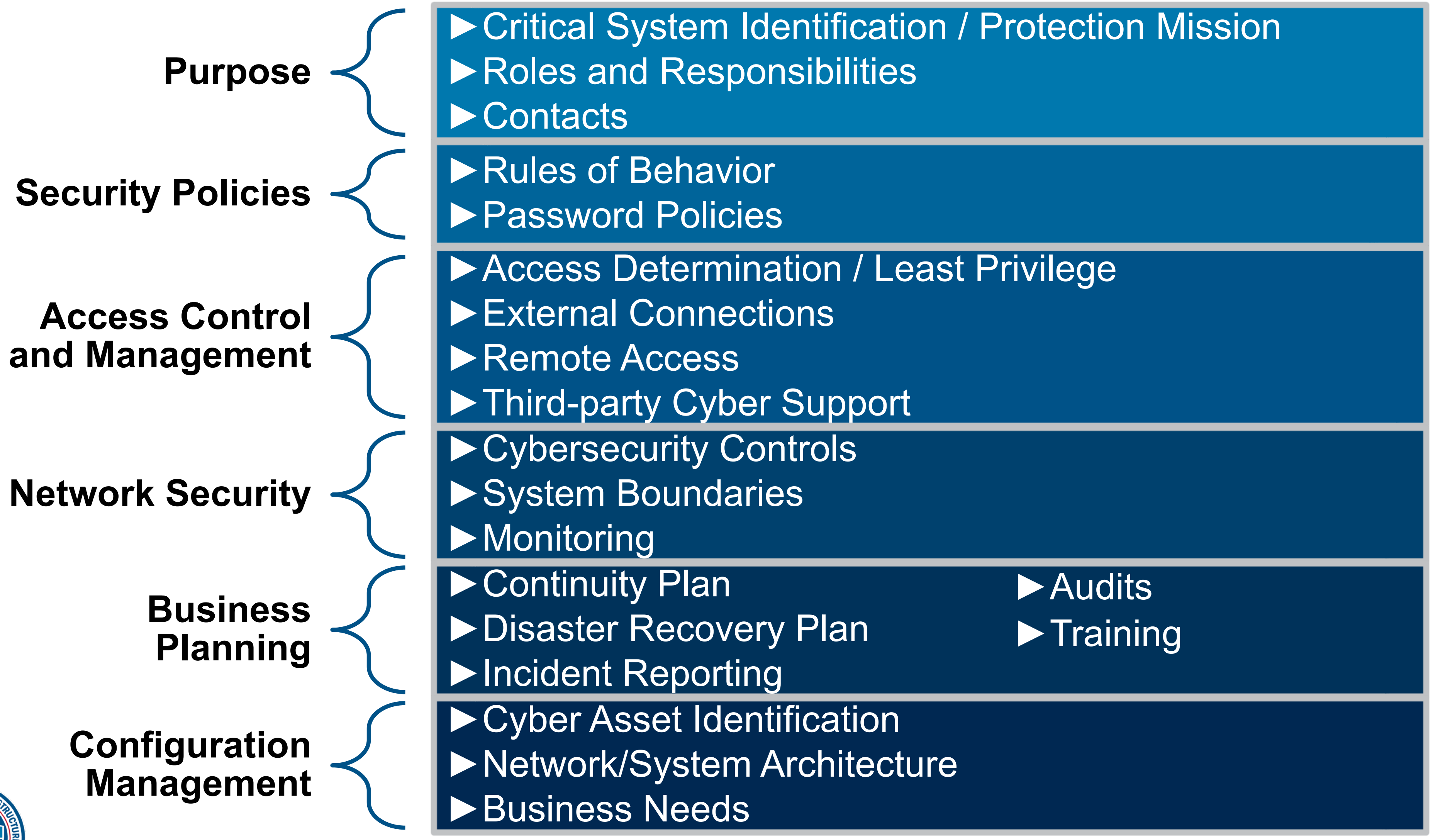
SERVICES
3,600
Increase of 4

VULNERABLE HOSTS
142
No Change
37% of hosts vulnerable

VULNERABILITIES
337
Decrease of 6

SAMPLE REPORT CARD (data not real). For illustrative purposes only.

Step 3: Identify Cybersecurity Measures and Policies



Purpose

▶ Critical System Identification / Protection Mission
▶ Roles and Responsibilities
▶ Contacts

Security Policies

▶ Rules of Behavior
▶ Password Policies

Access Control and Management

▶ Access Determination / Least Privilege
▶ External Connections
▶ Remote Access
▶ Third-party Cyber Support

Network Security

▶ Cybersecurity Controls
▶ System Boundaries
▶ Monitoring

Business Planning

▶ Continuity Plan
▶ Disaster Recovery Plan
▶ Incident Reporting
▶ Audits
▶ Training

Configuration Management

▶ Cyber Asset Identification
▶ Network/System Architecture
▶ Business Needs

Reporting Cyber Incidents

SHIELDS UP

- We have developed a webpage and fact sheet (cisa.gov/cfats-cyber-reporting) to help facilities determine how and when to report significant cyber incidents:
  - Examples of critical cyber systems
  - Examples of cyber incidents
  - Actions to take before, during, and after a cyber incident, including reporting
  - Additional resources and trainings

Note

This resource has no new reporting requirements but consolidates and clarifies existing requirements under RBPS 8 – Cyber and RBPS 15 – Significant Security Incidents.