

# THE EVOLUTION OF MALWARE & FUTURE MALWARE MITIGATION

Secure Delaware 2021



# Cybersecurity and Infrastructure Security Agency (CISA)

## VISION

Secure and resilient  
infrastructure for the  
American people.

## MISSION

CISA partners with industry and  
government to understand and  
manage risk to our Nation's  
critical infrastructure.



## OVERALL GOALS

### GOAL 1

#### DEFEND TODAY

Defend against urgent  
threats and hazards

seconds | days | weeks

















### GOAL 2

#### SECURE TOMORROW

Strengthen critical  
infrastructure and  
address long-term risks

months | years | decades

# 16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

 CHEMICAL	CISA	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	CISA	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	CISA	 GOVERNMENT FACILITIES	GSA & FPS
 CRITICAL MANUFACTURING	CISA	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	CISA	 INFORMATION TECHNOLOGY	CISA
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
 EMERGENCY SERVICES	CISA	 TRANSPORTATIONS SYSTEMS	TSA & USCG
 ENERGY	DOE	 WATER	EPA

# Sampling of Voluntary & No-Cost Cybersecurity Offerings

- **Assessments & Evaluations**

- Cyber Resilience Reviews (CRR™)
- Cyber Infrastructure Surveys
- Phishing Campaign Assessment
- Vulnerability Scanning & Web Application Scanning
- Risk and Vulnerability Assessments (aka “Pen” Tests)
- External Dependencies Management Reviews
- Cyber Security Evaluation Tool (CSET™)
- Validated Architecture Design Review (VADR)

- **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
- Workshops (Cyber Resilience, Cyber Incident Management, Election Security, etc.)

- **Partnership Development**

- Informational Exchanges
- Working Group Support

- **Strategic Messaging & Advisement**

- Resource Briefings
- Keynotes and Panels
- Threat Briefings
- Topic Specifics (e.g., NCSAM, SCRM, ICS, etc.)

- **Incident Response Assistance**

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination
- Targeted (Victim) Notifications



# Unique Critical Infrastructure in Delaware

## Financial

- 67.8% of Fortune 500 companies are Delaware entities
- Over 89% of all companies that held an IPO in 2019 were Delaware corporations
- Unique Court called the Court of Chancery

## Transportation

- Ranks #1 U.S. gateway for imports of fresh fruit & leading US seaport for cattle exports

## Food & Agriculture

- Ranks #1 nationally in the value of agricultural products sold per farm

## Critical Manufacturing

- Outfitted every American astronaut that has walked on the moon
- Global leader in the production of immediate-relief antacid actives and pharmaceutical industry

## Chemical

- One of the world's largest chemical companies

## Health

- Top 1% in Best Hospitals rankings



# What is Malware?

**Malware** is a collective name for all *malicious software* variants designed to cause damage to a computer, server, application, or network with malicious intent.

## Types of Malware:

- Viruses
- Worms
- Trojans
- Rootkits
- Hybrid (i.e., Botnets)
- Ransomware
- Spyware
- Adware



# The Evolution of Malware

## Experiment Era

The first viruses were developed in this era as innocent experiments. Initially, the programs were designed for research purposes.

Creeper Virus  
Reaper Program  
Brain Virus  
Morris Worm

1970-1988

## Cybercrime Era

The start of cyber criminality began. The World Wide Web was publicly launched, and virus developers realized that malicious programs could be profitable.

AIDS Trojan  
Computer Misuse Act  
Norton Antivirus  
World Wide Web  
Citibank Hack  
Concept Macro Virus  
Melissa Virus w/ Email Worm

1989-1999

## Internet Era

The Internet spread throughout the world and website hacks began to rise and started to cause more damage. This began the start of organizations developing guidelines and best practices.

ILOVEYOU Worm  
Ecommerce DDoS Attack  
PCI DSS  
Best Practices and  
Guidelines

2000-2005

# The Evolution of Malware – Continued

## Espionage Era

Digital attacks started to be used for spying and to cause physical disruption to governments and critical infrastructure. The first state-sponsored group started, and national security became a concern.

## Expansion Era

The rise of attacks resulted in loss of business, even bankruptcy. Zero-day, smart phone, aggressive social engineering attacks began to rise. Cyber attacks also began to interfere with political elections and altered public opinion via the spread of dis/mis/mal- information campaigns.

## Mainstream Era

Today most things on the Internet are interconnected and is a target for attack. Most entities deal with digital partnerships that host critical data and services. Malicious actors have widely adopted the use of vulnerabilities of digital partners to hack companies.

Storm Botnet  
MalCon Conference  
APT10  
Stuxnet

RSA / Yahoo / Facebook /  
Equifax / Marriott Hacks  
DNC Breach via WikiLeaks  
WannaCry Ransomware  
CCPA and GDPR

COVID-19 themed phishing  
FireEye / SolarWinds' Hack  
Colonial Pipeline Hack

Cloud

2006-2010

2011-2019

2020-Beyond



# “It’s All Connected” – Commercial Aviation Example



## Internet of Things (IoT) Applications:

Manufacturing process, predictive maintenance, inflight diagnostics, Wi-Fi, entertainment & dining

- *“The current A350 model has a total of close to 6,000 sensors across the entire plane and generates 2.5 Tb of data per day, while the newer model – expected to take to the skies in 2020 – will capture more than triple that amount.” – Data Science Central, 2015*
- *“There are 5,000 commercial aircraft in the sky at any one time over the US alone, and 35 million departures each year.” - Data Science Central, 2015*

NOTE: All of the content in the U.S. Library of Congress, the largest library in the world with more than 170 million items, is about 15 TB.

# Potential Future Impacts of Malware

Potential Future Impacts > Loss of Critical Data + Financial Loss + Damage to Reputation

- Water Treatment Tampering & Poisoning
- Blast Furnace Explosions
- Power Grids Blackout
- Safety System Failures (i.e., Cameras, Fire Alarms, Temperature Monitors, etc.)
- Loss of Life



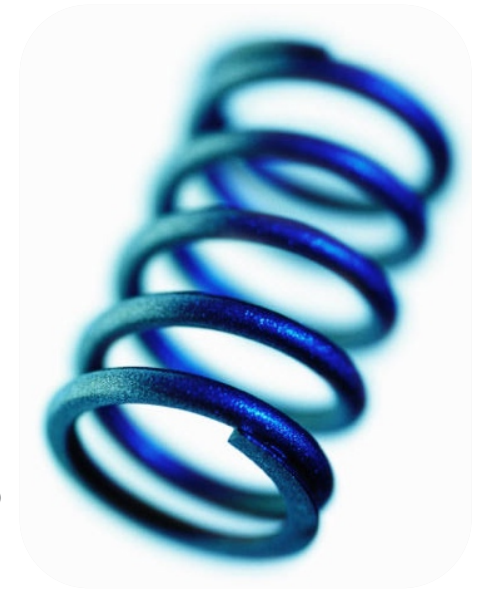
# What can we do to mitigate the potential impacts of malware?



# Build a Cyber Resilient Organization

*“... the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents...”*

- Presidential Policy Directive 21  
February 12, 2013



<b>Protect (Security)</b>	<b>Sustain (Continuity)</b>
<b>Perform (Capability)</b>	<b>Repeat (Maturity)</b>



# How Do I Become Cyber Resilient?

Cyber resilience emerges from what we do! We cannot buy it.

- The same way we achieve good health.
  - Exercising, eating right, getting enough sleep, getting routine check-ups, or seeking out specialist to help with specific issues
  - Avoiding risky behavior whenever possible
- Good health **emerges** from these activities! Similarly, operational resilience **emerges** from the activities we do.



# But I don't know where to start?



# Start with a Cybersecurity Assessment

**It all starts with an assessment. Then, a plan to secure your organization.**

- Take a holistic & hard look at your organization
- Evaluate the effectiveness of your cybersecurity controls, preparedness, and overall resilience
- Use your results as a baseline for moving forward
- Make it routine & keep it relevant with vulnerability trends and evolving adversarial activities



# CISA'S No-Cost Cybersecurity Assessments

Cyber Resilience Review (Strategic) -----

External Dependencies Management (Strategic) -----

Cyber Infrastructure Survey (Strategic) -----

Cybersecurity Evaluations Tool (Standards)-----

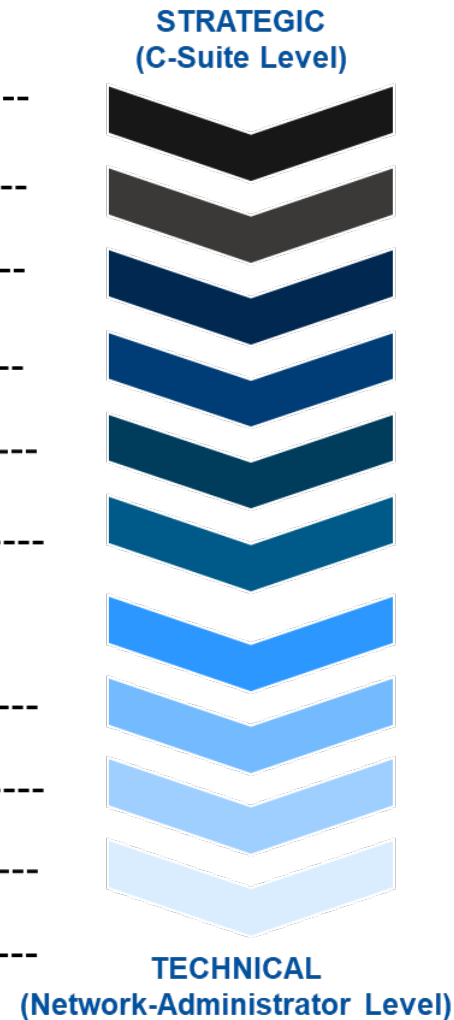
Phishing Campaign Assessment (EVERYONE) -----

Validated Architecture Design Review (Tactical) -----

Cyber Hygiene (Technical)

- Vulnerability Scanning -----
- Web Application Scanning -----
- Remote Penetration Test -----

Risk and Vulnerability Assessment (Technical) -----





# What can I do next?



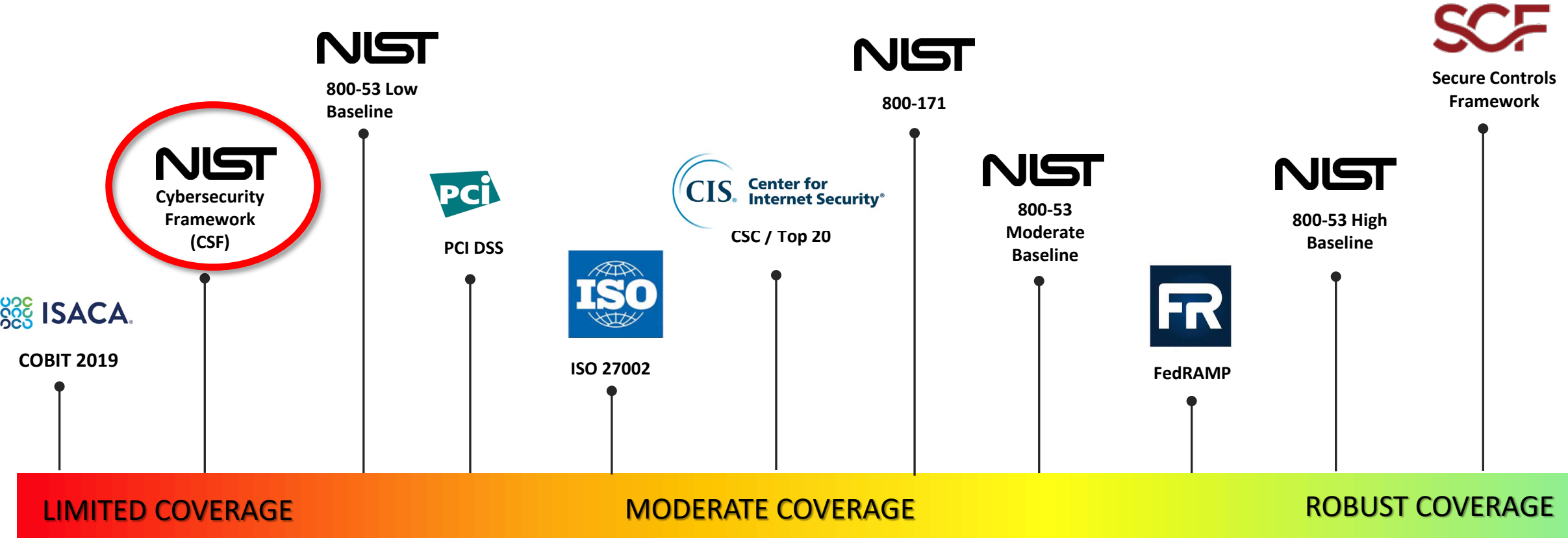
# Choose a Cybersecurity Framework that Best Fits Your Organization?

Picking a framework is more of a business decision and less of a technical decision.

- At minimum, select a framework that:
  - Aligns with the organization's business needs & meets risk-tolerance level
  - Reasonably meets expectations for security & privacy
  - Complies with applicable laws, regulations, and contractual obligations
  - Can the organization can implement within budget



# Common Cybersecurity Frameworks



# NIST Cybersecurity Framework (CSF)

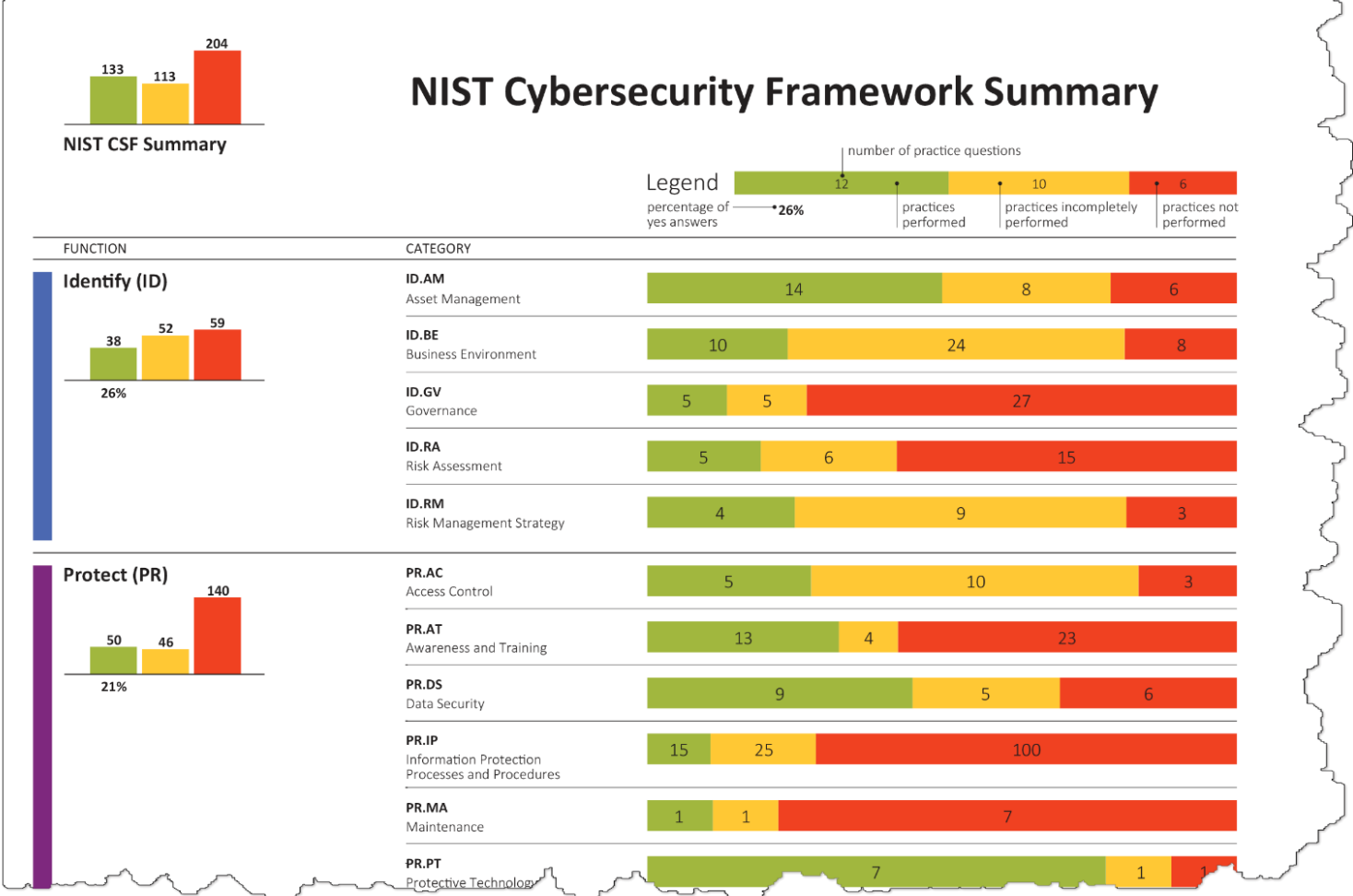
- Establishes a common perspective and vernacular,
- Provides risk-based guidelines,
- Is collaboration-oriented, and
- Is internationally recognized.

For more information, visit [nist.gov/cyberframework](https://nist.gov/cyberframework).

Functions	Categories
IDENTIFY (ID)	Asset Management (AM)
	Business Environment (BE)
	Governance (GV)
	Risk Assessment (RA)
	Risk Management Strategy (RM)
PROTECT (PR)	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processes and Procedures (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT (DE)	Anomalies and Events (AE)
	Security Continuous Monitoring (CM)
	Detection Processes (DP)
RESPOND (RS)	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
RECOVER (RC)	Improvements (IM)
	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)

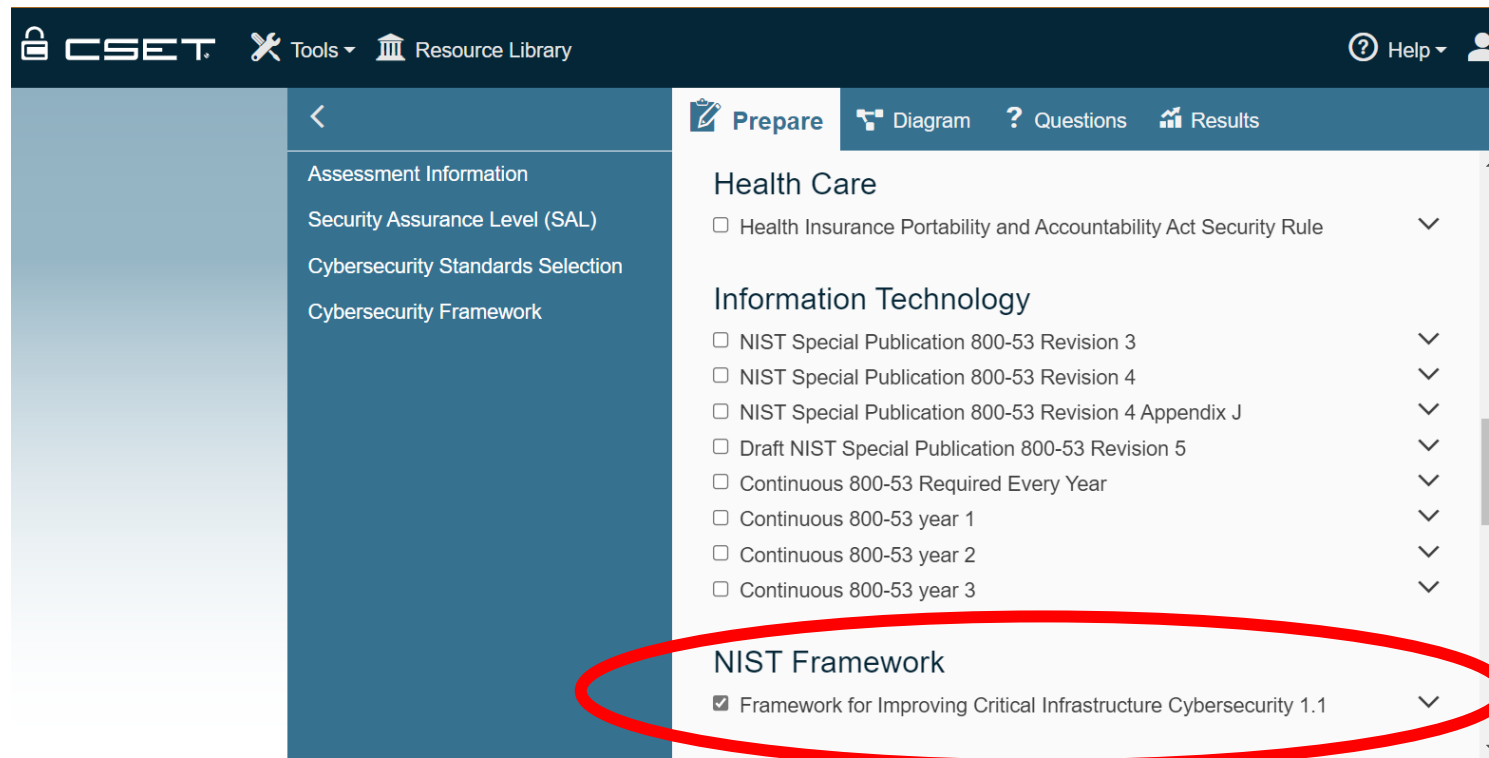


# NIST CSF Summary Report – Example from CRR



# Using the Cyber Security Evaluation Tool (CSET®) for NIST CSF

CSET® is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating Operational Technology and Information Technology.



# Another step in the right direction...

(More Technical & Complex)



# Moving Up the “Pyramid of Pain” using a Cyber Kill Chain Framework

- Kill Chain Frameworks help with the identification and prevention of cyber intrusions activity
  - Focuses on the tactics, techniques, and procedures used by attackers
- Tools and techniques can defeat most common computer network defense mechanisms

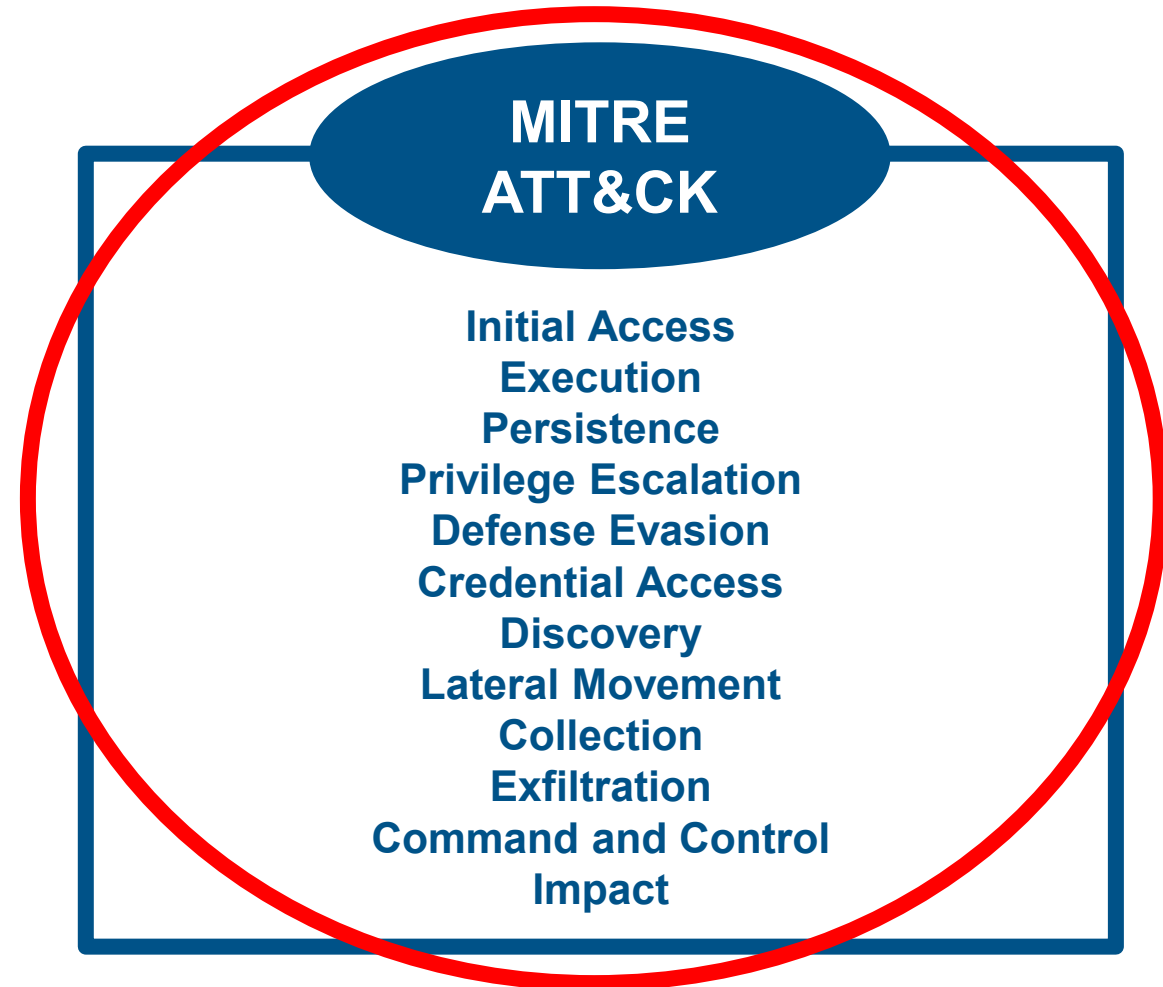




# Learn Attacker Tactics & Techniques using a Framework



VS



# MITRE ATT&CK Framework

- Knowledge base of adversary tactics and techniques based on real-world observations
  - Cyber threat intelligence coming from knowledge of past incidents, commercial threat feeds, information-sharing and threat-sharing programs
- Gives analysts a common language to communicate across reports and organizations
- Helps cyber defenders identify and detect the techniques used by an adversary and find capability gaps
- Visualizes how that adversary uses the techniques, as well as how you can potentially mitigate them



# MITRE ATT&CK Framework Sample

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Service Discovery
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Domain Policy Modification (2)	Execution Guardrails (1)	Modify Authentication Process (4)	Domain Trust Discovery
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Escape to Host	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Network Service Scanning
			User Execution (3)	Windows Management Instrumentation	External Remote Services	Hide Artifacts (7)	Steal Application	Network Share Discovery
					Hijack Execution Flow	Hijack Execution Flow (11)		Network Sniffing

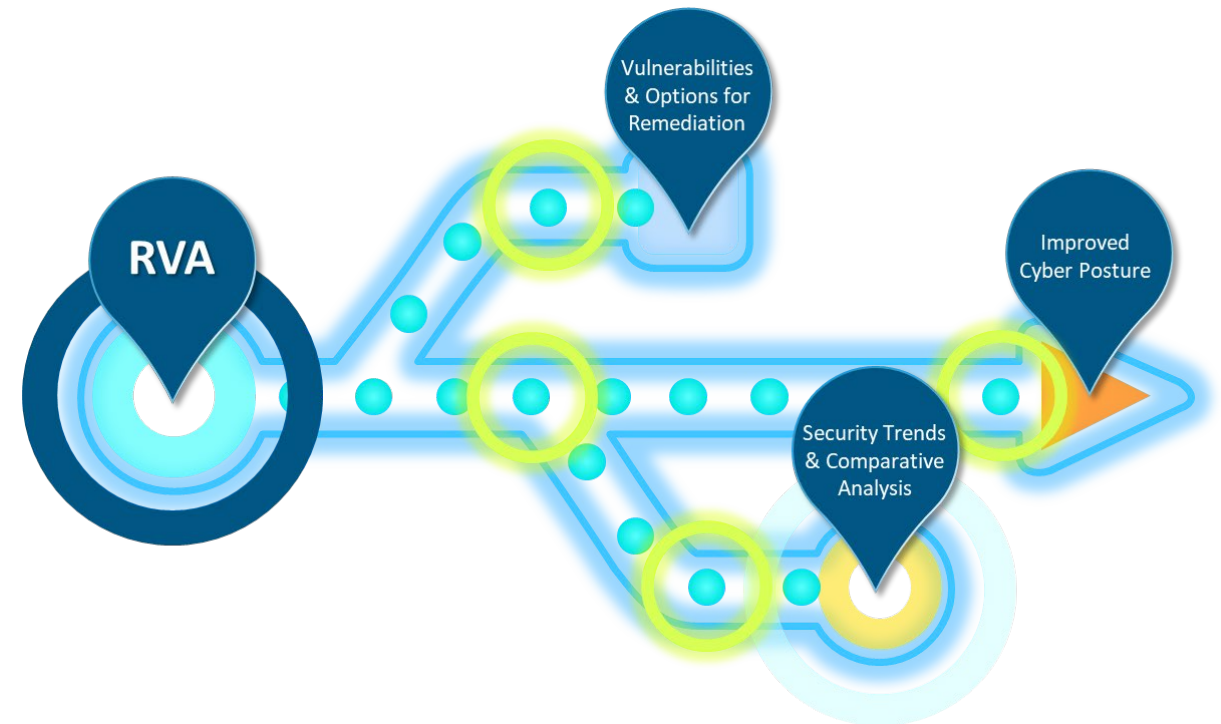


# But I don't have the resources to implement a Kill Chain Framework?



# Risk and Vulnerability Assessment (RVA)

- **Purpose:** Perform network penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks
- **Delivery:** Onsite by CISA
- **Benefits:**
  - Identification of vulnerabilities
  - Specific remediation options for improvements
  - Improves an entity's cyber posture, limits exposure, reduces rates of exploitation
  - Increases speed and effectiveness of future cyber attack responses
  - Discover security trends across all RVA stakeholder environments



# RVA Specifics

## Assessment Aspects

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness, test responses in systems, applications, network, and security controls
Social Engineering	Craft e-mail at targeted audience to test security awareness, used as an attack sector to internal network
Wireless Discovery & Identification	Identify wireless signals and 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



# CISA RVA Mapped to the MITRE ATT&CK Framework

1. In Fiscal Year 2020 (October 2019 to September 2020), CISA performed network penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks
2. After conducting the RVA, CISA mapped each technique to the MITRE ATT&CK Framework and noted the success rate for that technique across all assessments
3. Based on the results of 37 total assessments, CISA identified the top ten mitigations that are widely effective across the top techniques.



# Top 10 Mitigations from the RVA Results\*



## MITIGATIONS FOR TOP TECHNIQUES

The top ten mitigations shown here are widely effective across the top techniques.

### M1013 Application Developer Guidance

Provide secure software best practice guidance and training to application developers to avoid introducing security weaknesses through code.

### M1017 User Training

Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spear-phishing and social engineering.

### M1018 User Account Management

Manage the creation, modification, use, and permissions associated to user accounts.

### M1026 Privileged Account Management

Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.

### M1027 Password Policies

Set and enforce secure password policies for accounts.

### M1030 Network Segmentation

Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to sensitive systems and information.

### M1031 Network Intrusion Prevention

Configure Network Intrusion Prevention systems to block malicious file signatures and file types at the network boundary.

### M1042 Disable or Remove Feature or Program

Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

### M1049 Antivirus/Antimalware

Maintain Antivirus/Antimalware software up to date and configured to recognize and remove malicious files that have been downloaded or created on the host.

### M1051 Update Software

Periodically perform software updates, including vendor patches, OS updates, and firmware upgrades, to mitigate exploitation risk.



\*Top techniques and mitigations vary by sector and environment. Organizations should consider additional attack vectors and mitigation strategies based on their unique environment.



I already have a mature  
cybersecurity & cyber  
resilience posture. So,  
what else can I do?



# Cyberattack: Not If... But When

**Don't let your first time responding to an attack be the day of an actual incident!**

**IR First Responder Training**

**IR Readiness Review / Assessment**

**IR Program Development**

**IR Tabletop Exercise / Workshop**

- Bring all stakeholders to the table (i.e., external affairs / media team, human resources, network admins, CISO/CSO)
- Practice communications between information technology (IT) and operational technology (OT) and physical security and cybersecurity teams





**CISA**  
CYBER+INFRASTRUCTURE

**Arielle Baine**  
Cybersecurity Advisor, Region 3  
Delaware Cyber State Coordinator  
[Arielle.Baine@cisa.dhs.gov](mailto:Arielle.Baine@cisa.dhs.gov)

Regional Support:  
[CISARegion3@hq.dhs.gov](mailto:CISARegion3@hq.dhs.gov)

To Report an Incident:  
<https://us-cert.cisa.gov/report>

Media Inquiries:  
[CISAMedia@cisa.dhs.gov](mailto:CISAMedia@cisa.dhs.gov)



**CISA**  
CYBER+INFRASTRUCTURE