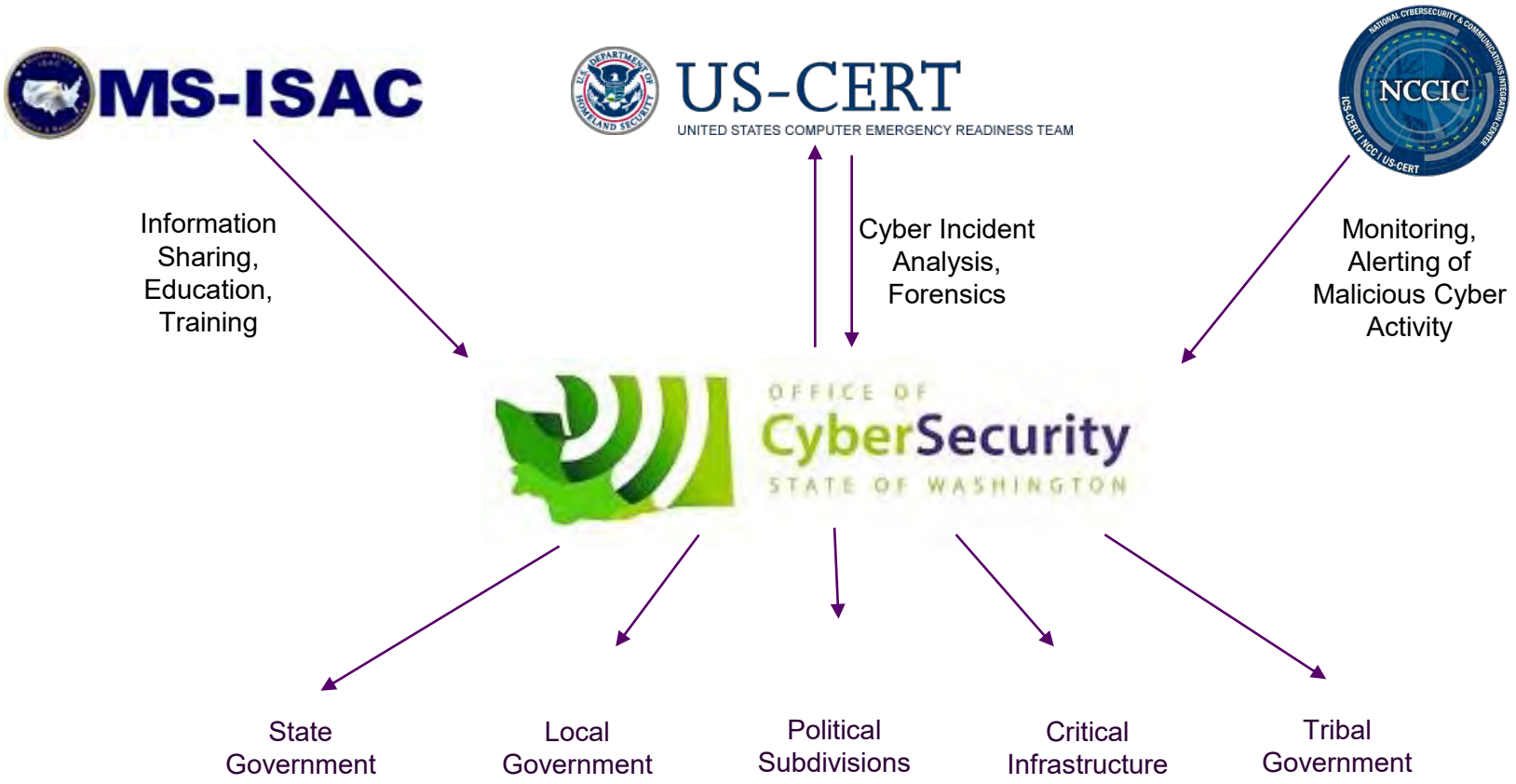
OFFICE OF
CyberSecurity
STATE OF WASHINGTON

Cyber Security Threats to State Government

David Morris, CTO
Office of CyberSecurity

Relationships



Our Approach

- What are we protecting?
- Who is the adversary?
- What methods to they use?
- Do I have the resources necessary to protect, detect and respond?

OFFICE OF CyberSecurity STATE OF WASHINGTON

Threat Actors

- Supply Chains
- Financial Services

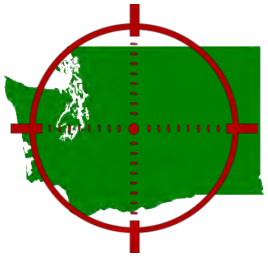
State-Sponsored

- High Capacity
- PII, Intellectual Property

Organized Crime

Hacktivists

- Cause-related
- Targets of Opportunity



Terrorist Group

- Sophisticated
- Critical Infrastructure

Petty Criminal

- Unsophisticated
- Opportunistic

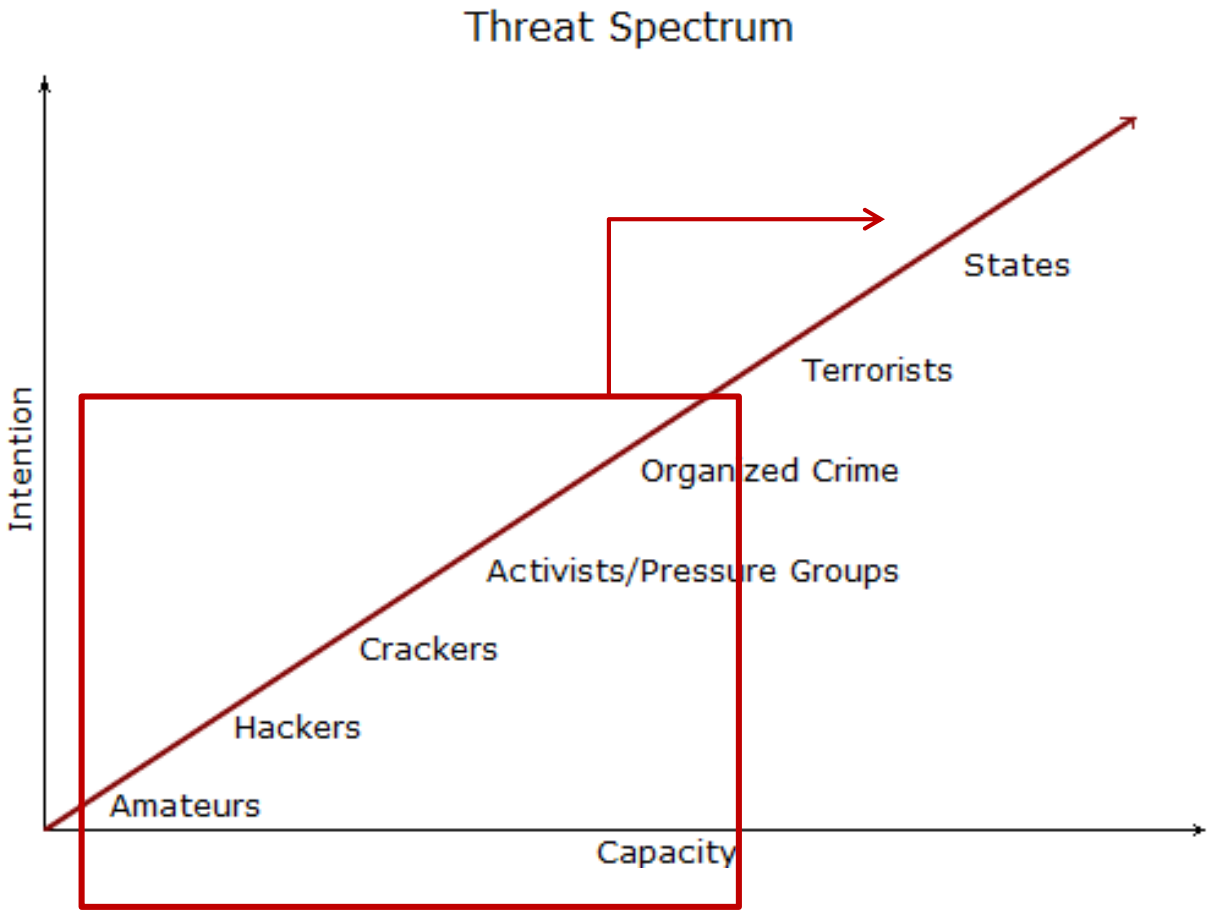
OFFICE OF CyberSecurity STATE OF WASHINGTON

Industry Threat Trends

- Increased Sophistication
  - Blurred line b/w State Sponsored and Petty Criminal
- Evolution of Ransomware
  - WannaCry & Petya
- Internet of Things (IoT)
- Targeted Phishing
- Cyber Fatigue / Malaise

OFFICE OF CyberSecurity STATE OF WASHINGTON

Increased Sophistication

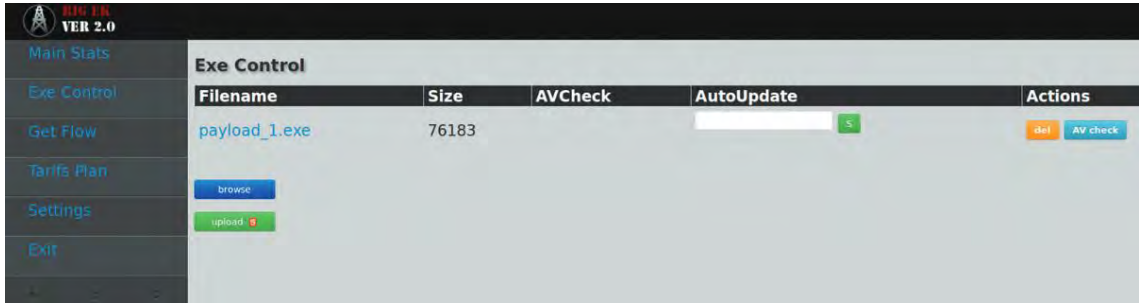


Malware as a Service

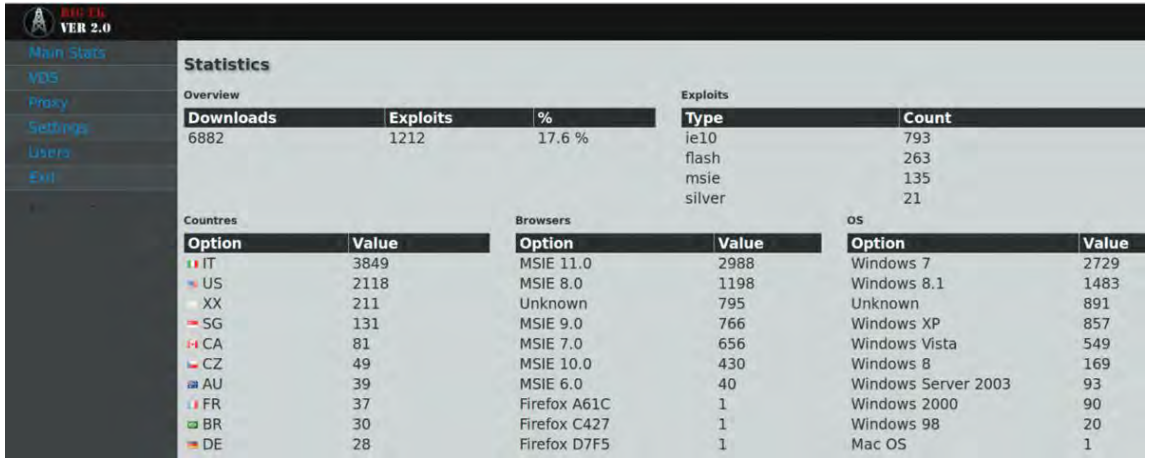
Malicious software packages to automate the exploitation of a target's vulnerabilities

Key characteristics:

- Designed for Novices
- Simple User Interface
- Packages Multiple Attacks

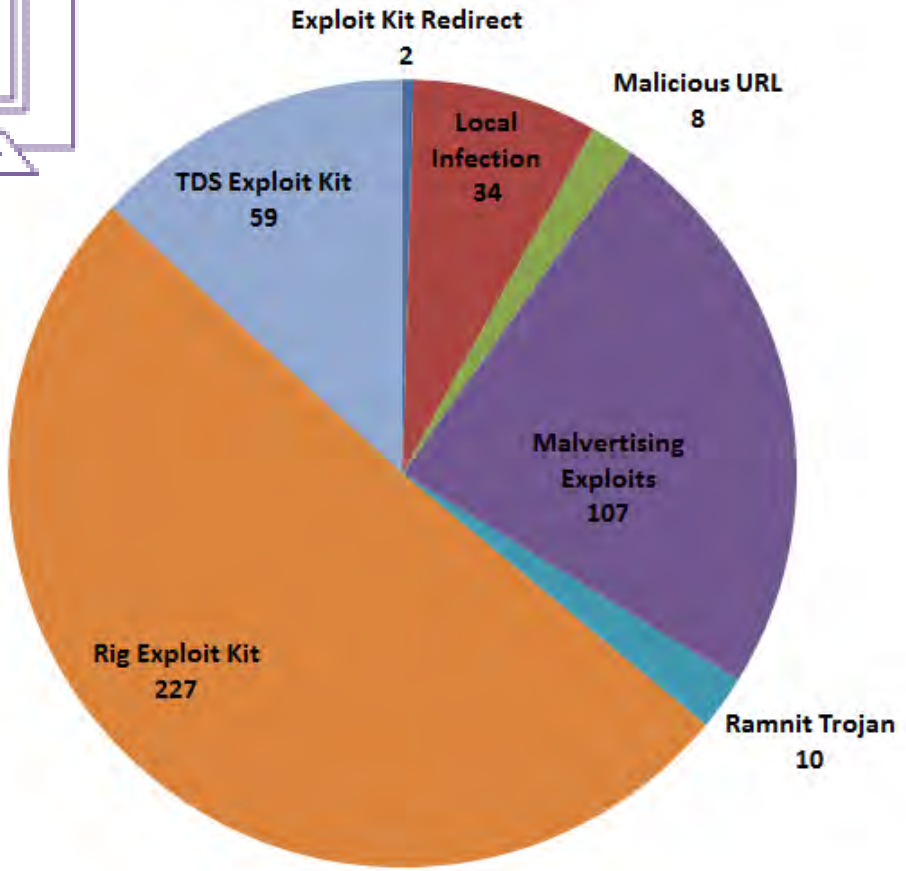


- Tech Support
- Performance Metrics



OFFICE OF CyberSecurity STATE OF WASHINGTON

Zero Day Detections – Past 120 Days



OFFICE OF
CyberSecurity
STATE OF WASHINGTON

Fun with Spam

James Veitch, TedTalk

WaTech
Washington Technology Solutions
"the consolidated technology services agency -RCW 43.105.006"

Security Operations Center

Past 30 Days:

- 67 Alerts
  - Malicious Software (32)
  - Investigations (9)
  - Account Compromise (13)
  - Probing (10)
  - Denial of Service (3)

CERT Capabilities

- Certified Incident Handlers
- FEMA Cyber Terrorist First Responders

- Digital Forensics Investigators
- Recognized Court Expert

- Malware Analysis
- Log Analysis
- Packet Analysis
- Root Cause Identification

OFFICE OF CyberSecurity STATE OF WASHINGTON

Response Roles

Incident Command Role

- OCS CERT acts as Incident Command, delegates tasks and communicates with agency leadership

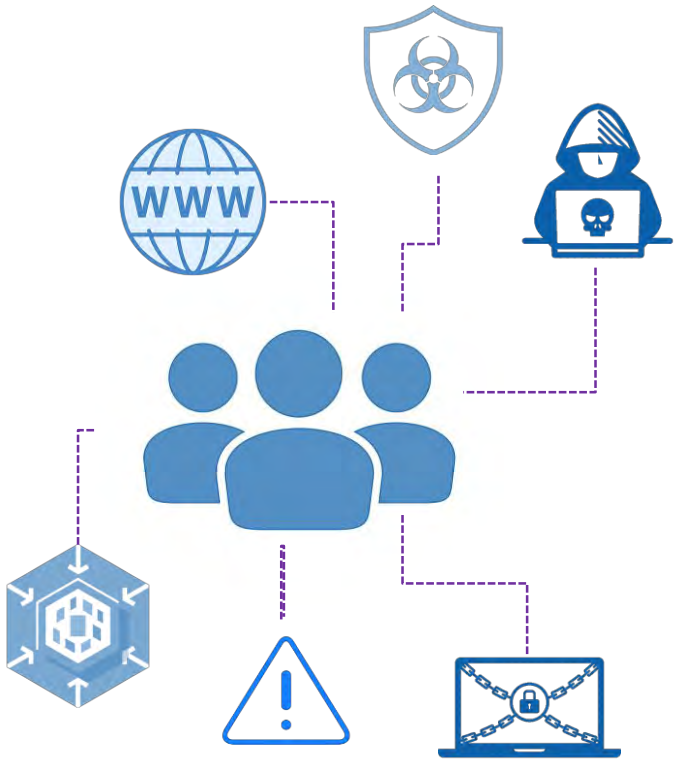
Agency Extension Role

- OCS CERT acts an extension of the agency incident response team

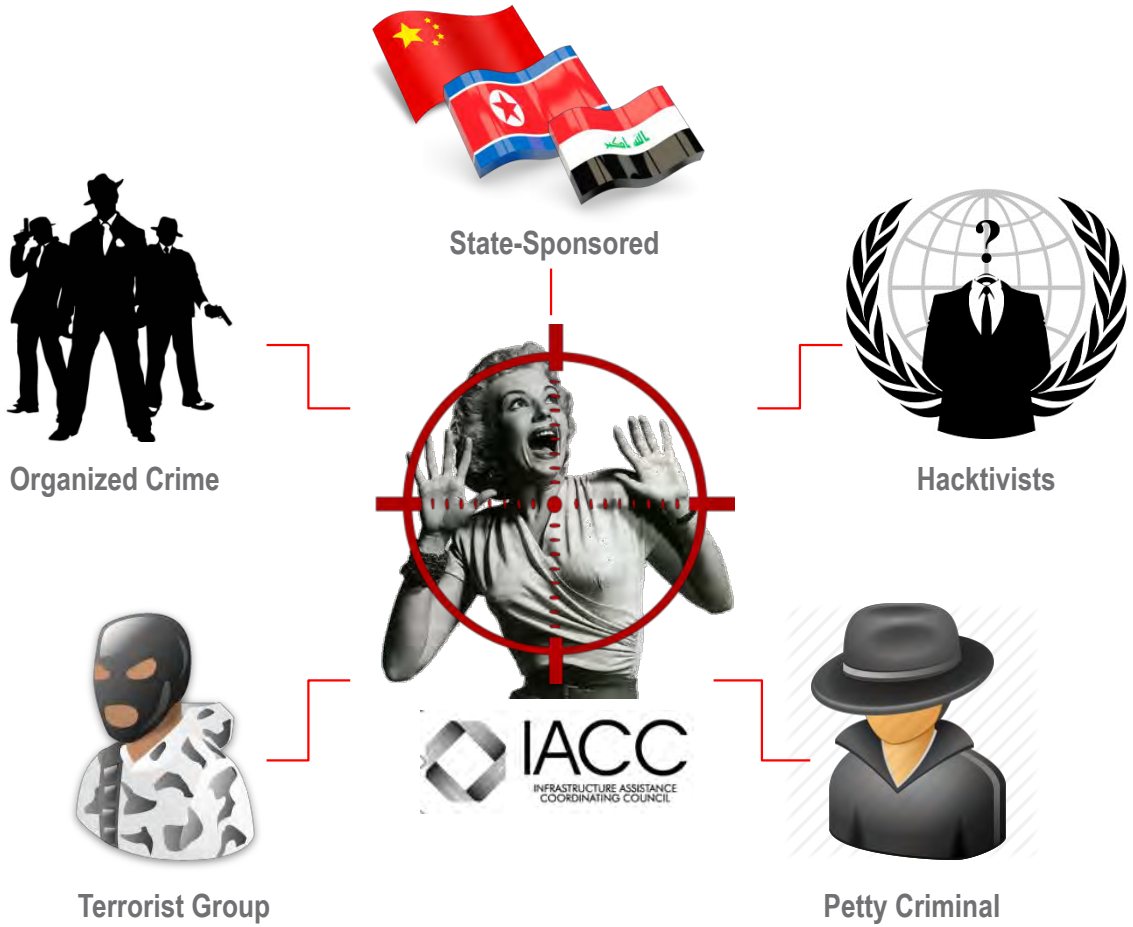
OFFICE OF CyberSecurity STATE OF WASHINGTON

Cases

- Site Defacements
- Credible Threats
- Data Breach
- Ransomware
- APT Activity
- System Compromise

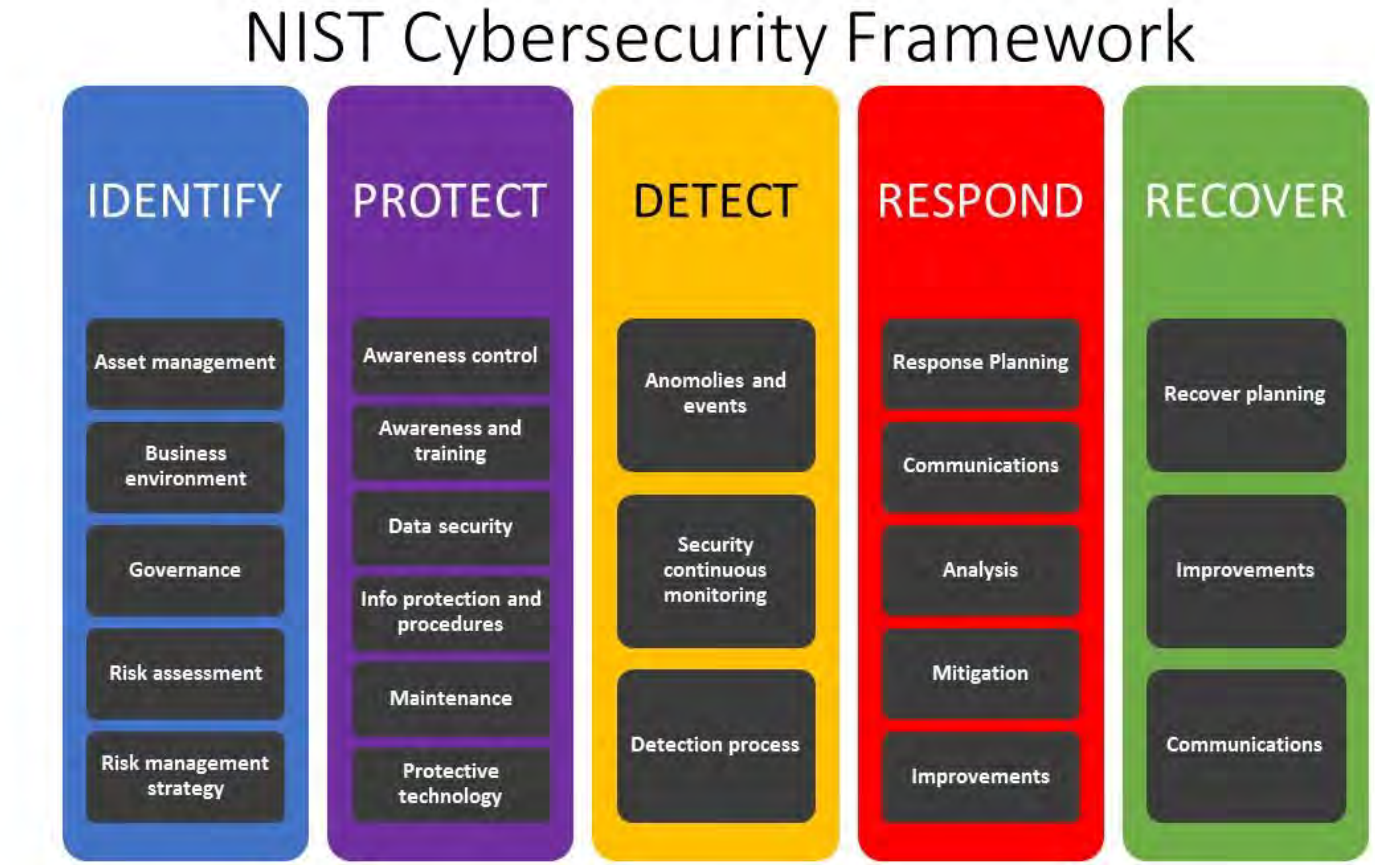


What can you do?



OFFICE OF CyberSecurity STATE OF WASHINGTON

Risk-Based Approach



Office of CyberSecurity
STATE OF WASHINGTON

Myths and Realities

IACC
INFRASTRUCTURE ASSISTANCE COORDINATING COUNCIL











OFFICE OF
CyberSecurity
STATE OF WASHINGTON

Defense in Depth

- Policy
- Patching
- Passwords
- Backups
- Endpoint Protection

Shared Responsibility

MS-ISAC

- 24/7 Security Operation Center and **Incident Response Services**
- Cybersecurity Advisories and Notifications
- Secure Portals for Communication and Document Sharing
- Cyber Alert Map
- Malicious Code Analysis Platform (MCAP)
- Weekly Top Malicious Domains/IP Report
- Monthly Members-only Webcasts
- Access to Cybersecurity Table-top Exercises
- Vulnerability Management Program (VMP)
- Nationwide Cyber Security Review (NCSR)
- Awareness and Education Materials

OFFICE OF CyberSecurity STATE OF WASHINGTON

Summary

- The state is attacked by multiple threat groups with different motives and capabilities
- Attack tools, techniques, and procedures are available to those with limited skills
- Shared responsibility and risk mitigation is critical to defense
- Spear Phishing is #1 delivery method for malicious software

Questions?