



# CITY OF HARRISONBURG

## CYBERSECURITY PROGRAM



## Traffic Light Protocol 2.0

The TLP is a set of designations that ensures that critical information is shared with the right people. It uses four colors to indicate the recipient's expected sharing limits, which are to be applied by them.

Here are the 4 LABELS

**TLP:RED**

LIMITED TO RECIPIENT ONLY- You can act on a TLP:RED cybersecurity document if you receive one, but you must not convey it to anyone else.

**TLP:AMBER**

LIMITED DISCLOSURE- This information can only be shared on a need-to-know basis among those within your organization and its customers.

The source may restrict sharing to the organization by setting TLP:AMBER+STRICT.

**TLP:GREEN**

LIMITED DISCLOSURE TO COMMUNITY- You may share this information within your community. The TLP leaves it up to you to be reasonable about which people constitute your community,

**TLP:CLEAR**

DISCLOSURE IS NOT LIMITED- Recipients can share this information with everyone.

# THIS PRESENTATION IS TLP: WHITE

---



# AGENDA

---

Cybersecurity Overview

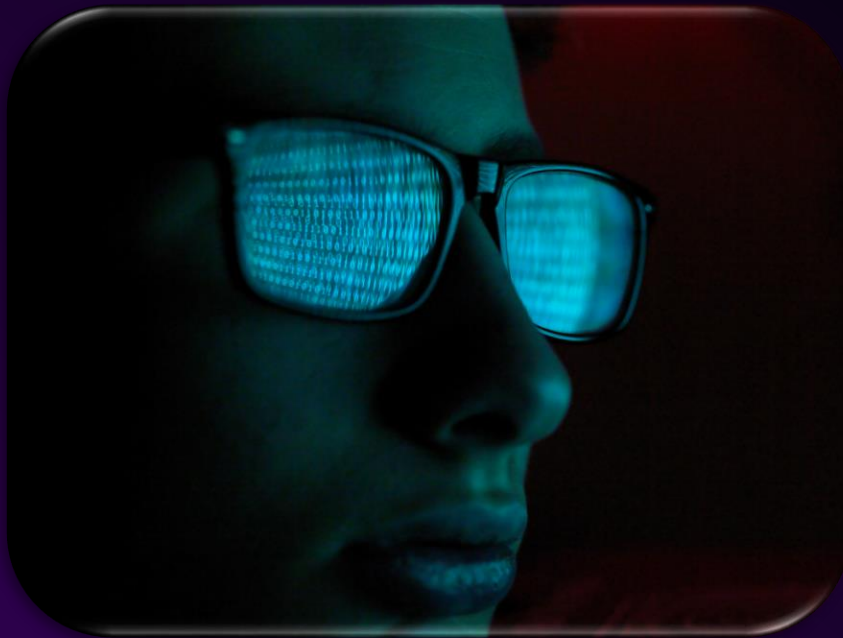
Program Accomplishments

Program Goals

Q&A

# THE REAL QUESTION: WHEN NOT IF

---



- Increasing number of local incidents
- Constant recon
- Daily phishing attempts
- Rise in ransomware attacks



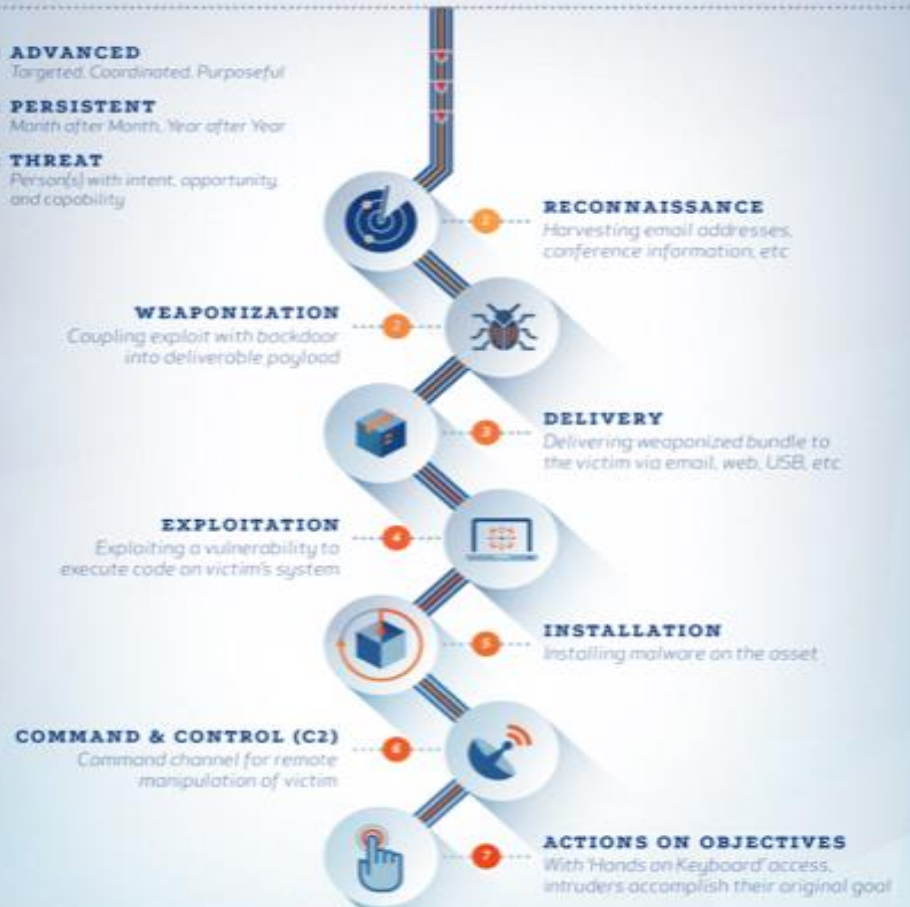
# CYBERSECURITY TERMS

- THREAT
- VULNERABILITY
- EXPLOIT
- RISK

## CYBER KILL CHAIN®

Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

- A : ADVANCED**  
Targeted, Coordinated, Purposeful
- P : PERSISTENT**  
Month after Month, Year after Year
- T : THREAT**  
Person(s) with intent, opportunity and capability



Learn how defenders have the advantage at:  
[lockheedmartin.com/cyber](http://lockheedmartin.com/cyber)



# CYBER THREAT INTELLIGENCE

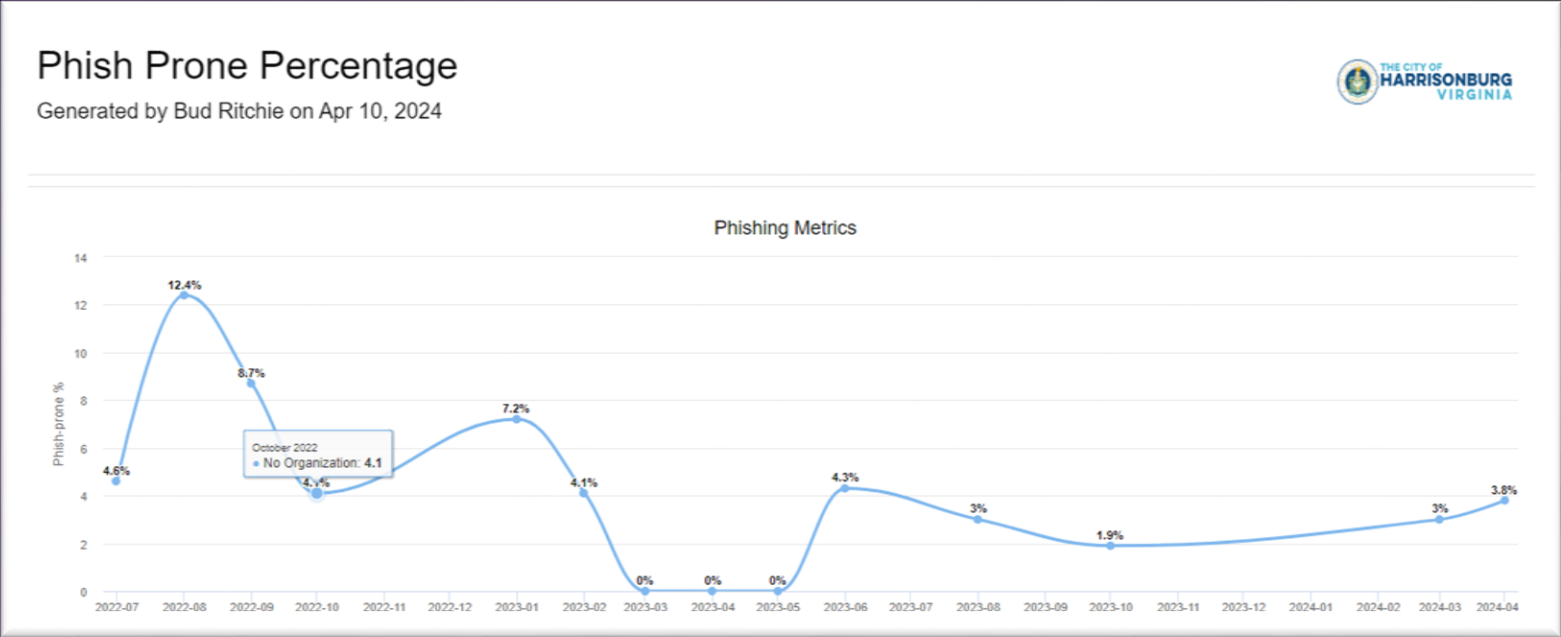
---

- MS-ISAC
- Regional Local Government Info Share
- Virginia Fusion Center (VSP)
- Verizon Data Breach Investigative Report (DBIR)
  - 74% of breaches involve a human factor
  - Compromised Credentials



# CYBER PROGRAM ACCOMPLISHMENTS

# HUMAN RISK MANAGEMENT PROGRAM



- In person training sessions
- Improved security culture
- Increase in phish reporting
- Decrease in phish prone percentage (12.3% to 3.8%)



# INTERNAL PENETRATION TEST

---

- Conducted over ten days June 2023
- Biggest areas of improvement
  - Password Policy
  - Vulnerability Management Program

# CYBER ASSET ATTACK SURFACE MANAGEMENT PROGRAM

---

- Identify and classify cyber assets
- Identify vulnerabilities
- Remediate vulnerabilities
- Process starts at acquisition and ends with disposal

# POLICY UPDATES

---

- Acceptable Use
- Bring Your Own Device
- Password
- Incident Response Plan

# SECURITY TOOLS

---

- Increased Network Visibility
- Vulnerability Scanner
- DARKTRACE

# ADDITIONAL ACHIEVEMENTS

---

- Staff tabletop scenarios
- Modernizing of infrastructure
- Payment Card Industry Data Security Standard (PCI DSS) Compliant



# GOALS

---

1. Consistent schedule for IT/Cybersecurity policy review
2. Cross train IT staff
3. Improvements to ICS/OT security
4. 24/7 Security Monitoring
5. Full alignment with NIST/CISA Cybersecurity Program Goals/Framework

## Long Term Goals

- Integrate Cyber into Business Continuity Plans
- Increase network visibility
- 3<sup>rd</sup> party vendor cybersecurity verification
- Passwordless Access

# TAKEAWAYS

---

- Increasing cyber resiliency
- Achievable goals
- Willing and receptive staff
- Team dedicated to keeping Citizen data safe and secure

# THANK YOU

---

Bud Ritchie

Cybersecurity and Compliance Specialist

[bud.ritchie@harrisonburgva.gov](mailto:bud.ritchie@harrisonburgva.gov)