VIRGINIA
CYBER SECURITY PARTNERSHIP

VIRGINIA CYBER SECURITY COMMISSION
November 7, 2014

Mission Statement

- The mission of the Virginia Cyber Security Partnership is to establish and maintain a trusted community of public and private sector cyber professionals. The Partnership leverages our collective experience and knowledge, promotes mutually beneficial information sharing and fosters professional development. This mission seeks to advance our nation's interests.

Background

- Formed in March 2012 in partnership with Richmond FBI
- Strategy
  - Trust is essential. Relationships are the foundation.
  - Control growth to ensure value and effectiveness
  - Promote participation of significant partners
  - Provide technical and managerial/executive offerings
- Currently a pilot for FBI National Program
- Partnering with ODNI / ISE
  - Planning two “federal day” executive sessions

Background

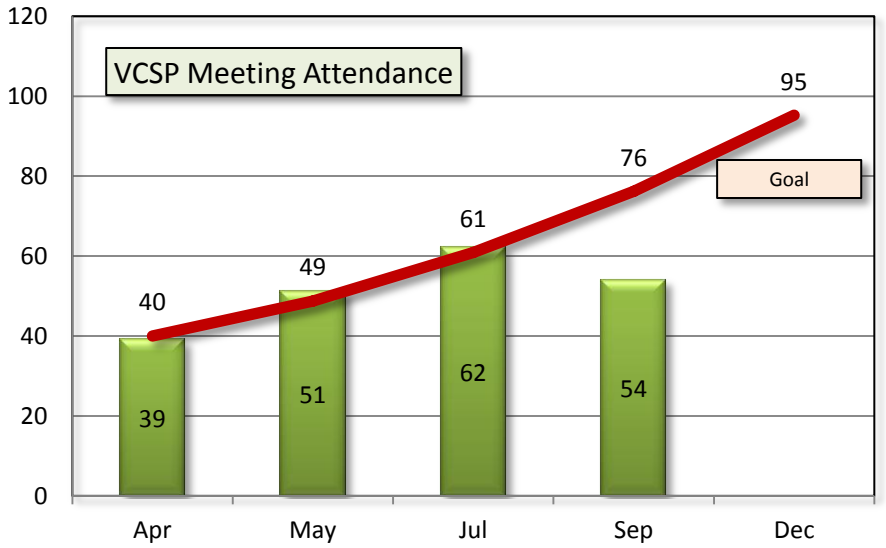
- Advisory Board
  - Establishes vision and mission
  - Sets strategic direction
  - Monitors progress towards defined objectives
  - Advocates for collaboration/sharing between members
  - Includes Dominion, VITA, Capital One, ePlus, Altria, Tata Communications and FBI

Mission Objectives

- Skills Enhancement
- Risk Management Best Practices
- Threat Information Sharing
- Resource Development Pipeline
- Community Outreach

2014 Goals

- Conduct 5 full membership meetings (Achieved)
- Conduct at least 2 meetings via WebEx and 1 from Virginia Tech (Achieved)
- Conduct group outreach activities at a minimum of 4 Virginia Colleges/Universities/High Schools. (Achieved)
- Track individual outreach activities as a metric of CSP community involvement. (Achieved)
- Increase participation in full membership meetings by 25% (In Progress)



Collaboration Framework

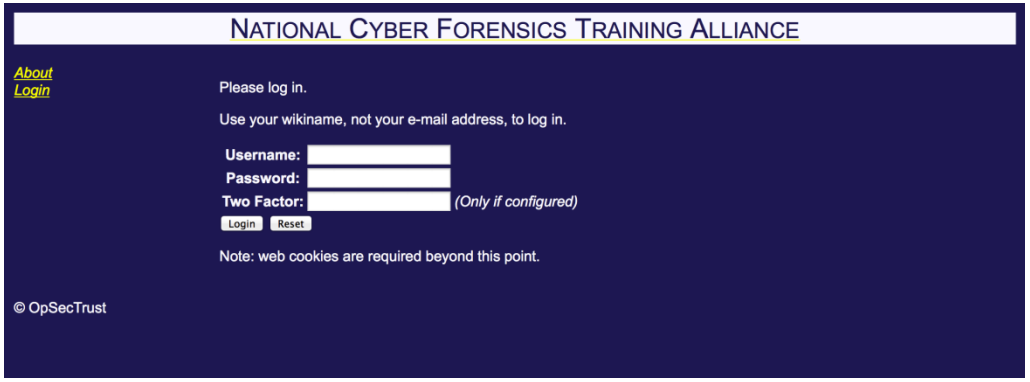
- **Themed Meetings**
  - Risk Management
  - Threat Intelligence
  - Protection of PII
  - Network Defense
  - Cyber Security and the Law
- **Lecture and Practical**
  - Presentations
  - Lab Exercises
  - Breakout Sessions
- **Dual Program Tracks**
  - CISO / Director level
    - Cyber Risk Leadership
  - CISO and below

Outreach Activities

- Deep Run High School (Henrico County) - Cyber Education Sessions
- Virginia Tech –Career Panel
  - 30 Students from CS, BIT and Engineering
  - Sophomores, Juniors and Seniors
- Longwood University - Career Panel (Nov 10)
- Numerous individual member speaking engagements

Secure Enclave

- Capabilities
  - Provides a trusted environment for further intelligence sharing and discussion
  - Infrastructure by the National Cyber Forensics and Training Center Alliance (NCFTA)
  - PGP Encryption Key for each CSP member
  - Email and Wiki functionality
  - Membership validation process
  - Platform to upload sensitive information (e.g., FBI PINs and Flashes)
  - Maintain membership participation
- Launches for all CSP members January 2015



Partnership Examples

- **Intelligence Provided**
  - 30+ Presentations provided to Private and Academic Sectors
  - Numerous FBI PINs and Flash Alerts distributed to CSP members
  - 5 Classified briefings for cleared CSP members
  - Threat Briefings at CSP meetings from:
    - FBI Cyber Division
    - FBI Cyber Initiative and Resource Fusion Unit (CIRFU)

- **Intelligence Response**
  - Compromise of employee PII (FBI Case Opened)
  - DDoS investigation (FBI Case Opened)
  - Unattributed APT actors compromised the web site of the Greek embassy in Beijing with a watering hole attack (FBI Case Opened)
  - Corporation provided information about expansion to China
  - Coordination with DHS on potentially compromised chipset

Questions?

Marc Gaudette
Chair – Virginia Cyber Security Partnership Advisory Board

Appendix

Mission Objectives

- **Skills Enhancement**

  Objective: Provide opportunities for the enhancement of skills and competencies
  - Continuing education sessions for CSP membership
  - Conduct “Capture the Flag” educational exercises
  - Provide hands-on training in cyber forensic analysis
  - Provide ethical hacking training
  - Other DHS sponsored training
  - Secure Development Lifecycle (SDLC) training

- **Best Practices**

  Objective: Share best practices in risk management and information assurance
  - Risk analysis and prioritization
  - Security awareness topics and techniques
  - Threat and incident management
  - Information protection
  - Secure Development Lifecycle / application development
  - Cyber security standards (e.g., SANS Top 20 Critical Controls)
  - Cyberlaw

Mission Objectives

- **Threat Information Sharing**

  Objective: Share insights regarding current cyber security threats and mitigation strategies
  - Prevention and Detection Strategies
  - Share threat intelligence gathering and analysis techniques and resources
  - Geo-political dynamics and cyber security

- **Resource Development Pipeline**

  Objective: Develop and implement strategies for recruitment of highly qualified security professionals
  - Intern matching
  - Curriculum review and community validation
  - Career roadmap development (career guidance and branding)

Mission Objectives

- **Community Outreach**

  Objective: Promote careers opportunities in cyber security and responsible on-line behaviors
  - High school and College/University level
  - Increase awareness of cyber security related career paths
  - Increase awareness of forums that can enable cyber security knowledge and skills development (e.g., U.S. Cyber Challenge)