Exploring a National Cyber Security Exercise for Community Colleges

Casey W. O'Brien
Co-PI, CyberWatch Center
Community College of Baltimore County
Baltimore, Maryland
:: CyberWatch
:: Current Cyber Exercise Landscape
:: CCDC
:: Mid-Atlantic CCDC
:: Cyber Skills Exercise Two-Year (CSX2Y)
:: Pilot
:: Next Steps
:: Q&A
:: What is CyberWatch

- NSF/ATE-funded Regional Center:
  - CW I: over $3 million for 4 years
  - CW II (continuation grant): over $2 million for 3 years
- Includes two- and four-year schools, private businesses, and government organizations
:: What is CyberWatch (con’t)

- **Mission**: improve the quantity and quality of the Information Assurance workforce - nationally
What is CyberWatch (con’t)

- Curriculum and faculty development
- K-12 initiatives
- Dissemination and outreach
- Internships, scholarships, career placements
What is CyberWatch (con’t)

- Articulation models
- Virtual Labs
- Job fairs
- Student competitions
:: Current Cyber Exercise Landscape

- World Skills
- Cisco:
  - NetRiders
  - Tiger Net Challenge
- Iowa State University Cyber Defense Competition
Current Cyber Exercise Landscape (con’t)

- US Cyber Challenge (USCC):
  - US Cyber Patriot
  - DC3 Digital Forensics Challenge
  - SANS NetWars
:: Current Cyber Exercise Landscape (con’t)
  ▪ Cyber Defense Exercise (CDX):
    ▪ Military academies
Current CE Landscape (con’t)

- Various CTFs:
  - USCC
  - UCSB Int’l
  - DefCon
- Collegiate Cyber Defense Competition (CCDC)
:: CCDC

- 6th year
- Hub and spoke model:
  - 9 regions (hoping to expand to 10)
- Defense-only
- Scoring: services, SLAs, Red Team, injects
- National CCDC: UTSA
:: Mid-Atlantic CCDC

- 6th year
- Qualifying/regional model
- Virtual & face-to-face competitions
- Complex infrastructure (e.g., VoIP/GSM integration, SCADA-lite, IPv6)
Mid-Atlantic CCDC (con’t)

- Public/private partnership:
  - CCBC and iSight Partners – formerly White Wolf Security
- Law enforcement component
Mid-Atlantic CCDC (con’t)

- Human element:
  - CEO/City Manager
  - Insider threat/SE
:: Mid-Atlantic CCDC (con’t)

- Corporate sponsorship:
  - Boeing
  - CSC
  - Northrop Grumman
  - SAIC
  - Solera Networks
  - Tenable Network Security
:: Cyber Skills Exercise Two-Year (CSX2Y)

- Ultimate goals:
  - Get students psyched about IA
  - Create a pool of talent to meet national demand
  - Provide an educational experience first; gaming exercise second
:: CSX2Y (con’t)

- Ultimate goals (con’t):
  - Provide a way for schools to assess the effectiveness of their curricula
  - Create a spectator-friendly sport (e.g., ESPN, Cyber Security League)
:: CSX2Y (con’t)

- Rules:
  - Eligibility requirements that favor CC students
  - Rotating Rules committee
  - Division model
:: CSX2Y (con’t)

- Scoring:
  - Service availability
  - Flags captured
  - SLAs
  - Red Team
  - Scenarios
  - 3 Vs: visual, visual, visual
:: CSX2Y (con’t)

- Competition Models:
  - Virtual
  - Face-to-face
  - Blended virtual/F2F
  - CTF
:: CSX2Y (con’t)
  ▪ Competition Models (con’t):
    ▪ Defense-only
    ▪ Offense
    ▪ Blended defense/offense
    ▪ Quiz Bowl
:: CSX2Y (con’t)

- Competition Models (con’t):
  - Incident response
  - Engineering and implementation
:: CSX2Y (con’t)

- Preparation:
  - Prep guide
  - Cyber Security Clubs
  - Part of curriculum
  - Pickup-games (virtual)
  - Weekly exercises mapped to skills (virtual)
:: CSX2Y (con’t)

- Sustainability:
  - Entrance fees
  - Grants (NSF supplemental grant)
  - Corporate sponsorship
  - Product placement
:: CSX2Y (con’t)
  ▪ Sustainability (con’t):
  ▪ Advertisements
  ▪ Scholarships
  ▪ Ties into Marketing spoke
:: CSX2Y (con’t)

- Marketing:
  - National Cyber Security Student Association (in the works)
  - Conferences
  - Student Clubs at CCs
  - Word-of-mouth
  - NSF/ATE centers
:: CSX2Y (con’t)

- Marketing (con’t):
  - Sponsors
  - Press Releases
  - Social networking
  - Micro-site
:: CSX2Y (con’t)

- Recruiting:
  - Corporations
  - Government
  - Academia
:: CSX2Y (con’t)

- Curriculum:
  - Provides a way to measure the effectiveness of curriculum
  - New module development
  - Ties into Evaluation spoke
:: CSX2Y (con’t)

- Products & Services:
  - Products:
    - Vendors beta-testing their solutions
    - Vendors products integrated into competition (e.g., Solera, Tenable, Core)
  - Ties into Curriculum, Evaluation, Marketing, Sustainability spokes
:: CSX2Y (con’t)

- Products & Services (con’t):
  - Services:
    - Lab environment setup
    - Curriculum development
    - Faculty development
  - Ties into Marketing, Sustainability spokes
CSX2Y (con’t)

- Research:
  - Use infrastructure as data collection engine
  - Distribute data to academia/gov’t for free
  - Distribute data to commercial organizations for fee (e.g., JHU APL)
:: CSX2Y (con’t)

- Research (con’t):
  - Ties into Marketing, Product, Sustainability spokes
:: CSX2Y (con’t)

- Evaluation:
  - Scenario development tied to external standards (e.g., industry best practices, ISC² CBK, CNSS 40xx)

- Effectiveness:
  - Curriculum
  - Competitions
  - Skills
:: Pilot

- 09/18/10:
  - Center for Systems Security and Information Assurance (CSSIA)
  - Cal Poly Pomona
  - CyberWatch Center
- Virtual
:: Pilot (con’t)

- Competition model TBD (most likely CTF-based with Red Team)
- Stress-test virtual infrastructure
- Write-up/disseminate lessons learned
:: Next Steps

- Recruit CCs
- Develop Cyber Security League (CSL)
- Create a competition schedule
- Create desired skills matrix
- Create scenarios based on skills matrix
Next Steps (con’t)

- Incorporate Quiz Bowl, engineering, and implementation aspects
- Combine virtual competitions with face-to-face-based exercises:
  - Helps reduce structural and resource-related costs as well as entry costs
Next Steps (con’t)

- Explore 24-hour competitions
- Explore offensive component:
  - Develop student Red Teams
- Encourage law enforcement participation (e.g., Secret Service)
- Continue to work on the spectator aspects
:: Next Steps (con’t)

- Formalize sponsorship structure
- Continue to capture lessons learned
- Present findings at various conferences
:: Q&A

:: www.CyberWatchCenter.org

:: www.MidAtlanticCCDC.org

The CyberWatch Center is funded by the:

[NSF National Science Foundation logo]