Design and Launch of an Intensive Cybersecurity Program for Military Veterans

William D. Armitage
William Gauvin
Adam Sheffield

University of South Florida

FLORIDA CENTER FOR CYBERSECURITY
Demand & Supply

• Is there a real need for more cybersecurity operators?

OMB Memorandum, July 12, 2016

“The vast majority of Federal agencies cite a lack of cybersecurity and IT talent as a major resource constraint that impacts their ability to protect information and assets. There simply is not a sufficient supply of cybersecurity talent to meet the increasing demand of the Federal Government.”
Demand & Supply

• What’s the Supply?
  • Higher Education
    - 4-year degrees
    - 2-year degrees
    - certificate programs
  • “Career (vocational) schools” – often for profit
    - strong focus on industry certifications
  • Certification programs: “Buy this book”
  • Some specialized programs.
Higher Education

• Factors gumming up the cyber supply chain...
  • 4 (or even 2) years is often “too long”
  • Significant attrition in these programs
    - students deciding field is “not right for them”
    - little attention paid to determining suitability for the field
• Yet... higher ed. courses better for long-term
  - depth of understanding provides adaptability to changing technologies.
A possibly “suitable” source of talent?

Military veterans

• Unemployment numbers
  – Worse for recent conflicts

• Real problem: “UNDEREMPLOYMENT”
  – Highly motivated to fulfill responsibilities
  – For “combat specialties,” relatively few civilian job want ads fit this group.
Pointed out that military combat concepts such as perimeter defense are very similar to concepts one finds in cybersecurity defense, and may serve as a good foundation for cyber work.
As of 2014, there were “no programs designed to inform veterans of the value that their current skills in security can bring to the cyber field or augment those skills through training to address potential technical barriers to success in the cyber domain.”
The Players

• Florida Center for Cybersecurity (FC²)
  – Created in July, 2014 by Florida legislature
  – Based at the University of South Florida (USF)
• JP Morgan Chase
  – Global financial services firm
  – Had initiative, “New Skills at Work”, and also a strong interest in veteran employment
  – In September, 2014, contacted FC² to express interest in cybersecurity education
• USF’s Department of Computer Science & Engineering
• $300K proposal submitted by FC² in early 2015
  – Quickly funded, leading to...
The Program

NEW SKILLS FOR A NEW FIGHT
Recruitment & Selection

• Outreach
  – Social Media: Facebook & LinkedIn
  – Print advertising: local
    • Including MacDill AFB newspaper
  – Information Sessions
    • Press releases to local media

• Applicants invited to group sessions
  – Industry, academic and FC² personnel
  – Substituted for individual interviews.
Rubric Criteria

• The veteran’s military specialty code
  – Preference given to technical specialties
• Resume – any higher ed or other training
• Evaluation of a written personal statement
  – Often revealed motivation
• Score on a basic “computer knowledge” quiz
• Evaluation of letters of recommendation
• A subjective “commitment” rating.
Of note...

- 20 selected, plus a few on a waiting list
- Process “rank-blind”
  - Final participants all from enlisted grades
    - One commissioned and one warrant officer initially selected but withdrew prior to start of program
- “Over-qualified” applicants
  - Already had taken the four academic courses part of the program, or had equivalent knowledge
  - Put on different kind of waiting list.
Program Design

Three phases:

1. An academic base (16 weeks)
   - Dedicated classroom/lab
   - Program-only cohort

2. Intensive cybersecurity training (10 weeks)
   - Same classroom/lab & cohort

3. SOC internship (remainder of program)
   - Placed with industry partners
Phase 1: Academic Base

- Four pre-existing academic courses, from the Department’s online BSIT program
- Delivered in classroom mode in a dedicated facility to a cohort of military veterans.
Phase 1: Academic Base

• Advantages of using existing courses:
  
  – Courses count toward requirements of the BSIT, for students who wish to complete a degree later
  
  – Satisfactory completion earns the student a Foundations of Cyber Security certificate.
Phase 1:

**Course 1:** CGS 1540: Intro to Databases for IT
- Freshman/sophomore level introduction to databases
- MS Access 2010 & 2013, SQL language

**Course 2:** COP2510: IT Programming Fundamentals
- Sophomore level introduction to programming
- Focus placed on problem solving and program design using the Python programming language.
Phase 1:  

**Course 3**: CGS3303: IT Concepts  
- Junior level required course in BSIT program  
- Emphasizes “demystification of the computer,” plus covers topics such as history of computing, theory, number systems, networking, operating systems and machine language

**Course 4**: CIS3213: Foundations of Cyber Security  
- Junior level elective course in Cybersecurity.
Phase 1: ACADEMICS

STATS

• 20 students began Phase 1 in January, 2016
• 18 students completed
• 2 students who did not complete were offered IT-related jobs at strong starting salaries

• 2 open slots filled in from “overqualified” waiting list
• 20 students proceeded to Phase 2.
Program Design

Three phases

1. An academic base (16 weeks)
   Dedicated classroom/lab
   Program-only cohort

2. Intensive cybersecurity training (10 weeks)
   Same classroom/lab & cohort

3. SOC internship (remainder of program)
   Placed with industry partners
Phase 2: Intensive Cyber Training

• Three primary components
  – CSX Nexus Practitioner Training
  – Capstone Competitive Experience
  – Industry Certifications
Phase 2: Intensive Cyber Training

- CSX Practitioner Training
  - Performance-based certification
  - Virtual Lab environment
  - Three curriculum levels (includes NICE framework):
    - Identification & Protection
    - Detection
    - Respond & Recover.
Phase 2: Intensive Cyber Training

• Capstone Competitive Experience
  – Red Team / Blue Team Competition
    • Veterans staffed Blue team
    • University’s Whitehatters Computer Security Club staffed Red team.
Phase 2: Intensive Cyber Training

• Industry Certifications
  — Assisted Self-study
    • CompTIA Security+
    • CompTIA Network+
  — Scenario-based testing
    • CSX Practitioner.
Phase 2: Intensive Cyber Training

**STATS**

- Began Phase 2 with 20 students
  - Two filled in from the “overqualified” waiting list.
- 19 completed
- Certification testing became available August 1\(^{st}\), and continues during Phase 3.
Program Design

Three components

1. An academic base (16 weeks)
   - Dedicated classroom/lab
   - Program-only cohort

2. Intensive cybersecurity training (10 weeks)
   - Same classroom/lab & cohort

3. SOC internship (remainder of program)
   - Placed with industry partners
Phase 3: Internships

• Paid
• Presentations during Phases 1 & 2
• “Resume book” provided to likely internship hosts
• Students applied and interviewed
• In progress; terminates on November 11th (Veterans’ Day).
Phase 3: Internships

STATS – as of today

- Of 19 in this phase:
  - 8 in active internship
  - 10 have been hired into fulltime positions
  - 1 declined internship and is instead in self-directed study for certifications.
Implementation Notes

• New facility constructed for program
  – Twenty Mac laptops + large-screen displays
  – LCD projector
  – Electronic podium
  – Four wall-mounted flat panel monitors

• Phase 1 instruction was Mon-Wed & Tue-Thu

• Two of four instructors were veterans

• TA’s assisted “across the board”

• Choice of S/U (12.5%) or A-F grading (87.5%).
Lessons Learned

• Student financial support
  – Ensure GI Bill can be used

• More Phase 1 course content coordination

• Increase networking course content

• Offer “pre-program” online coursework
  – Useful in selection, enhances base of knowledge

• Modify selection criteria
  – Include individual interviews
  – Give “points” for combat specialty codes.
Recommendations for Replicators

- Expand the wait list concept
- Equip the facilities early
- Consider combat specialty codes
- Use veterans as instructors
- Include individual interviews during selection
- Consider “pre-program” courses
- Take wounded warriors into account
- Encourage acceptance of responsibility.
Final Thoughts

• Program a success
  – Provided 19 entry-level cybersecurity operators
  – Timeframe of just over 10 months
  – 19 veterans will likely have more meaningful employment
  – Students have expressed satisfaction

• Provided a good base for future improvements

• Plans are to scale up and re-launch in 2017.
Contact Info

• Interested in more information, or in replicating this project?

• Contact:  **Adam Sheffield**  
  Associate Director  
  Florida Center for Cybersecurity  
  4202 E. Fowler Avenue, ISA7020 | Tampa, FL 33620-7120  
  Office 813-974-1869 | asheffie@usf.edu  
  [www.thefc2.org](http://www.thefc2.org)

• Or sign up to receive information.
Design and Launch of an Intensive Cybersecurity Program for Military Veterans

William D. Armitage
William Gauvin
Adam Sheffield

University of South Florida

FLORIDA CENTER FOR CYBERSECURITY
Phase 1: CGS 1540: Intro to Databases for IT

Course 1: CGS 1540: Intro to Databases for IT

• Freshman/sophomore level introduction to databases

• Content:
  – High-level knowledge of databases and their use
  – High-level knowledge required to design and build efficient databases
  – High-level knowledge of the use of MS Access 2010 & 2013 to create and manage databases.
  – High-level knowledge of the SQL query language.
Phase 1: ACADEMICS

**Course 2:** IT Programming Fundamentals (COP2512)

- Sophomore level introduction to programming
- Focus placed on problem solving and program design using the Python programming language.
- Primary topics:
  - problem solving
  - program design
  - Implementation
  - testing and debugging.
Phase 1: 

**Course 3:** CGS3303 IT Concepts

- Junior level course in BSIT program, taught online since 2007
- A “drill-down” course, covering “demystification of the computer,” plus other topics:
  - History of computing
  - Number systems
  - Theory
  - Computer logic
  - Networking
  - Operating systems
  - Cybersecurity
  - Assembly & Machine Language
Phase 1: Course 4: CIS3213 Foundations of Cyber Security

- Junior level course in Cybersecurity. Objectives:
  - Adversary analysis, common vulnerabilities, and attack techniques
  - Model cyber-attack phases and find active adversary activity
  - Perform aggregation and report cyber-attack information
  - Apply resources available for analysis of indicators and malware
  - Apply languages to define a cyber-attack for a specific environment
  - Use Cyber Threat Information Sharing (CTIS) methods
  - Perform as an active member of a Security Response Team at all levels.