Webinar Series

The Underserved Cybersecurity Workforce: Securely Provisioning our Future

October 10, 2018
National Cyber Security Awareness Month

• October is #cyberaware month
• Week 2: Oct. 8–12: Millions of Rewarding Jobs: Educating for a Career in Cybersecurity
• For more information, see:
  
  NIST National Cyber Security Awareness Month

  National Cyber Security Alliance
  https://StaySafeOnline.org/ncsam

  U.S. Department of Homeland Security
  https://dhs.gov/ncsam
NICE Cybersecurity Workforce Framework
NIST Special Publication 800-181
Reference Resource for Cybersecurity Workforce Development

• Audiences
  Public and Private Sector Employers
  Education Providers
  Technology Developers
  Current and Future Cybersecurity Workers
  Training and Certification Providers
  Policymakers

• Cybersecurity Workforce Categories (7)
  SECURELY PROVISION
  OPERATE AND MAINTAIN
  OVERSEE AND GOVERN
  PROTECT AND DEFEND
  ANALYZE
  COLLECT AND OPERATE
  INVESTIGATE

• Specialty Areas (33) – Distinct areas of cybersecurity work
• Work Roles (52) – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific Knowledge, Skills, and Abilities (KSA’s) required to perform a set of Tasks.
Category: Securely Provision

• Description: Conceptualizes, designs, procures, or builds secure information technology (IT) systems, with responsibility for aspects of system or network development.

• Specialty Areas, include:
  - Risk Management
  - Systems Requirements Planning
  - Systems Development
  - Test and Evaluation
  - Technology R&D
  - Systems Architecture
  - Software Development
Cybersecurity Supply/Demand Heat Map

Cybersecurity talent gaps exist across the country. Closely looking at these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

National level

<table>
<thead>
<tr>
<th>TOTAL CYBERSECURITY JOB OPENINGS</th>
<th>SUPPLY OF CYBERSECURITY WORKERS</th>
<th>GEOGRAPHIC CONCENTRATION</th>
<th>TOP CYBERSECURITY JOB TITLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>301,873</td>
<td>Very Low</td>
<td>National average</td>
<td>Cyber Security Engineer</td>
</tr>
<tr>
<td>TOTAL EMPLOYED CYBERSECURITY</td>
<td>CYBERSECURITY WORKFORCE</td>
<td>National average</td>
<td>Cyber Security Analyst</td>
</tr>
<tr>
<td>WORKFORCE</td>
<td>SUPPLY/DEMAND RATIO</td>
<td></td>
<td>Network Engineer / Architect</td>
</tr>
<tr>
<td>768,096</td>
<td>NATIONAL AVERAGE</td>
<td></td>
<td>Cyber Security Manager /</td>
</tr>
<tr>
<td></td>
<td>2.5</td>
<td></td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td>Geographic Concentration</td>
<td></td>
<td>Systems Engineer</td>
</tr>
<tr>
<td></td>
<td>Average Location Quotient</td>
<td></td>
<td>Software Developer / Engineer</td>
</tr>
<tr>
<td></td>
<td>National average</td>
<td></td>
<td>Vulnerability Analyst /</td>
</tr>
<tr>
<td></td>
<td>1.0</td>
<td></td>
<td>Penetration Tester</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Systems Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IT Auditor</td>
</tr>
</tbody>
</table>
JOB OPENINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY

- Operate & Maintain: 194,224
- Securely Provision: 181,601
- Protect & Defend: 121,752
- Analyze: 119,392
- Oversee & Govern: 87,038
- Collect & Operate: 48,314
NICE Framework Categories

SECURELY PROVISION

OPERATE AND MAINTAIN

OVERSEE AND GOVERN

PROTECT AND DEFEND

ANALYZE

COLLECT AND OPERATE

INVESTIGATE
Rethinking Cybersecurity from the Inside Out

An Engineering and Life Cycle-Based Approach for Achieving Trustworthy Secure Systems

Dr. Ron Ross
Computer Security Division
Information Technology Laboratory
Complexity.
The \( n + 1 \) vulnerabilities problem.

*Unconstrained due to increasing attack surface.*
The hard cybersecurity problems are buried below the water line...

In the hardware, software, and firmware.
For bridge builders, it's all about physics—

Equilibrium, static and dynamic loads, vibrations, and resonance.
For information system developers, it's all about mathematics, computer science, architecture, and systems engineering—

Trustworthiness, assurance, penetration resistance and resilience.
Reducing susceptibility to *cyber threats* requires a multidimensional systems engineering approach.

- **Harden the target**
- **Limit damage to the target**
- **Make the target survivable**

Security Architecture and Design

Achieving Trustworthiness and Resiliency
NIST Special Publication 800-160

Systems Security Engineering

Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
Security.

*An emergent property.*
Technical Processes

- Business or mission analysis
  - Stakeholder needs and requirements definition
    - System requirements definition
      - Architecture definition
      - Design definition
    - System analysis
      - Implementation
      - Integration
  - Verification
  - Transition
  - Validation
    - Operation
    - Maintenance
  - Disposal

Systems and software engineering — System life cycle processes
Nontechnical Processes

- Project planning
- Project assessment and control
  - Decision management
  - Risk management
    - Configuration management
    - Information management
    - Measurement
      - Quality assurance
    - Acquisition and Supply
    - Life cycle model management
  - Infrastructure management
- Portfolio management
- Human resource management
- Quality management
- Knowledge management

Systems and software engineering — System life cycle processes
Security should be a by-product of good design and development practices – integrated throughout the system life cycle.
Race to the Top

Better Security Through Engineering
Q & A
Cybersecurity Criticality is Driven by Increased Software

Carol Woody, Ph.D.
Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM18-1161
Software Reliance is Rapidly Expanding


From 1997 to 2012, software industry production grew from $149 billion to $425 billion
Software is Communicating to Other Systems

- Cellular
  - Main processor
  - Graphics processor
  - Base band processor (SDR)
  - Secure element (SIM)

- Automotive
  - Autonomous vehicles
  - Vehicle to infrastructure (V2I)
  - Vehicle to vehicle (V2V)

- Industrial and home automation
  - 3D printing (additive manufacturing)
  - Autonomous robots
  - Interconnected SCADA

- Aviation
  - Next Gen air traffic control
  - Fly by wire

- Smart grid
  - Smart electric meters
  - Smart metering infrastructure

- Embedded medical devices
Demand Drives Faster and Cheaper Approaches

Collective development – context:
- Too much specialization for one organization
- Too little value in individual components
- Each component is a decomposition of code collected from sub-components, commercial products, open source, code libraries, etc.
- Each collects, stores, and sends data in different file structures and formats using frameworks handle target infrastructure

Development is now assembly and reuse is rampant

Note: hypothetical application compositions
84% of Security Breaches Exploit the Software Applications

Breaking this cycle will require engineering of the software we use to handle the realities of the operational environment. All fielded software needs good cybersecurity. However,

- “76% of U.S. developers use no secure application program process”\(^3\)
- “More than 40% of software developers globally say that security isn't a top priority for them”\(^4\)

1. Clark, Tim, Most cyber Attacks Occur from this Common Vulnerability, Forbes. 03-10-2015
2. Feiman, Joseph, Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves, Gartner. 09-25-2014. G00269825
Anyone Can Write Software but is it Good?

How To Raise The Next Zuckerberg: 6 Coding Apps For Kids
http://readwrite.com/2013/04/19/how-to-raise-the-next-zuck-6-coding-apps-for-kids/

TYNKER - We Empower KIDS to Become Makers
https://www.tynker.com/

How and Why to Teach Your Kids to Code

Best-in-class code:  <600 defects per MLOC
Very good code:  600 to 1,000 defects per MLOC
Average quality code:  6000 defects per MLOC
Up to 5% of defects are vulnerabilities
Software Assurance Education for Improved Cybersecurity
Software Assurance Curriculum Project

Goals: Develop software assurance curricula
Define transition strategies for implementation

Community Outreach
- 20+ Published Papers
- 7 SEI reports
- 15+ talks, webinars, podcasts, media
- Thousands of downloads
- LinkedIn group of 500+ members
- Course materials and videos

Integrated into course offerings
- Carnegie Mellon University
- Stevens Institute of Technology
- US Air Force Academy
- University of Detroit Mercy
- University of Houston
- (ISC)

Transition
- Degree offerings
  - MSwA Curriculum Design:
    - Polytechnic University of Madrid
  - Community College Programs:
    - Illinois Central College
    - Alamo Colleges
    - Lincoln Land Community College
  - SwA Courses
    - Assurance Management
    - Assured Software Dev'T
    - Exec Course

https://www.sei.cmu.edu/education-outreach/curricula/software-assurance/index.cfm
Many Disciplines Need Software Assurance Knowledge

In Education and Training, Software Assurance could be addressed as:

• A “knowledge area” extension within each of the contributing disciplines;
• A set of functional roles, drawing upon a common body of knowledge; allowing more in-depth coverage dependent upon the specific roles.
Publication to Support the Curriculum

Cyber Security Engineering
A Practical Approach for Systems and Software Assurance

Nancy R. Mead
Carol C. Woody

Released November 2016 as part of the SEI Book Series

For more information see
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=483667
CERT Cybersecurity Engineering and Software Assurance Professional Certificate

Released March 2018

The program consists of five components

- Software Assurance Methods in Support of Cybersecurity Engineering
- Security Quality Requirements (SQUARE)
- Security Risk Analysis (SERA)
- Supply Chain Risk Management
- Advanced Threat Modeling

To learn more, visit https://sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=33881.
Two chapters are included in Engineering Emergence to be released January 2019 highlighting “Engineered to be Secure” and “Cyber Insecurity is Growing” for systems of systems.

SEI webpage for cybersecurity and software assurance: www.sei.cmu.edu/go/cybersecurity-engineering
Q & A
Report to the President on Growing and Sustaining the Nation’s Cybersecurity Workforce

Recommendations:

• The Executive Branch should strongly encourage educators, training providers, and employers to use the taxonomy and lexicon of the NICE Framework as the reference for building workforce development strategies.

• The federal government should partner with the private sector and academia to develop interdisciplinary cybersecurity curriculum guidance that addresses the need for widely accepted and shareable cybersecurity curricula that incorporate employers’ cybersecurity needs.

https://nist.gov/nice/cybersecurityworkforce
Goal 5: Increase awareness and education across the ecosystem

Actions:

• Government should encourage the academic and training sectors to fully integrate secure coding practices into computer science and related programs.

• The academic sector, in collaboration with the National Initiative for Cybersecurity Education, should establish cybersecurity as a fundamental requirement across all engineering disciplines.
National Apprenticeship Week
November 12-18, 2018

dol.gov/apprenticeship/naw/

National Cybersecurity Career Awareness Week
November 12-17, 2018

nist.gov/nice/nccaw
Thank You for Joining Us!

**Upcoming Webinar:** “Upskilling and Reskilling the Workforce for Cybersecurity Roles”

**When:** Wednesday, November 14, 2018 at 2:00pm – 3:00pm EST


[https://nist.gov/nice/webinars](https://nist.gov/nice/webinars)