Solving Cybersecurity Skills Shortage With Apprenticeships and Certifications

NDIA

20th Annual Systems Engineering Conference

Girish Seshagiri

19734

Topics

- Why We Are Here
- Ubiquitous Software Defects, “Patch and Pray”, What is at Stake
- Swiss/German Dual Track “Learn and Earn” Model
- DoL Registered Apprenticeships
- Community Initiative Center of Excellence for Secure Software (CICESS)
- Takeaways and “ASKs”

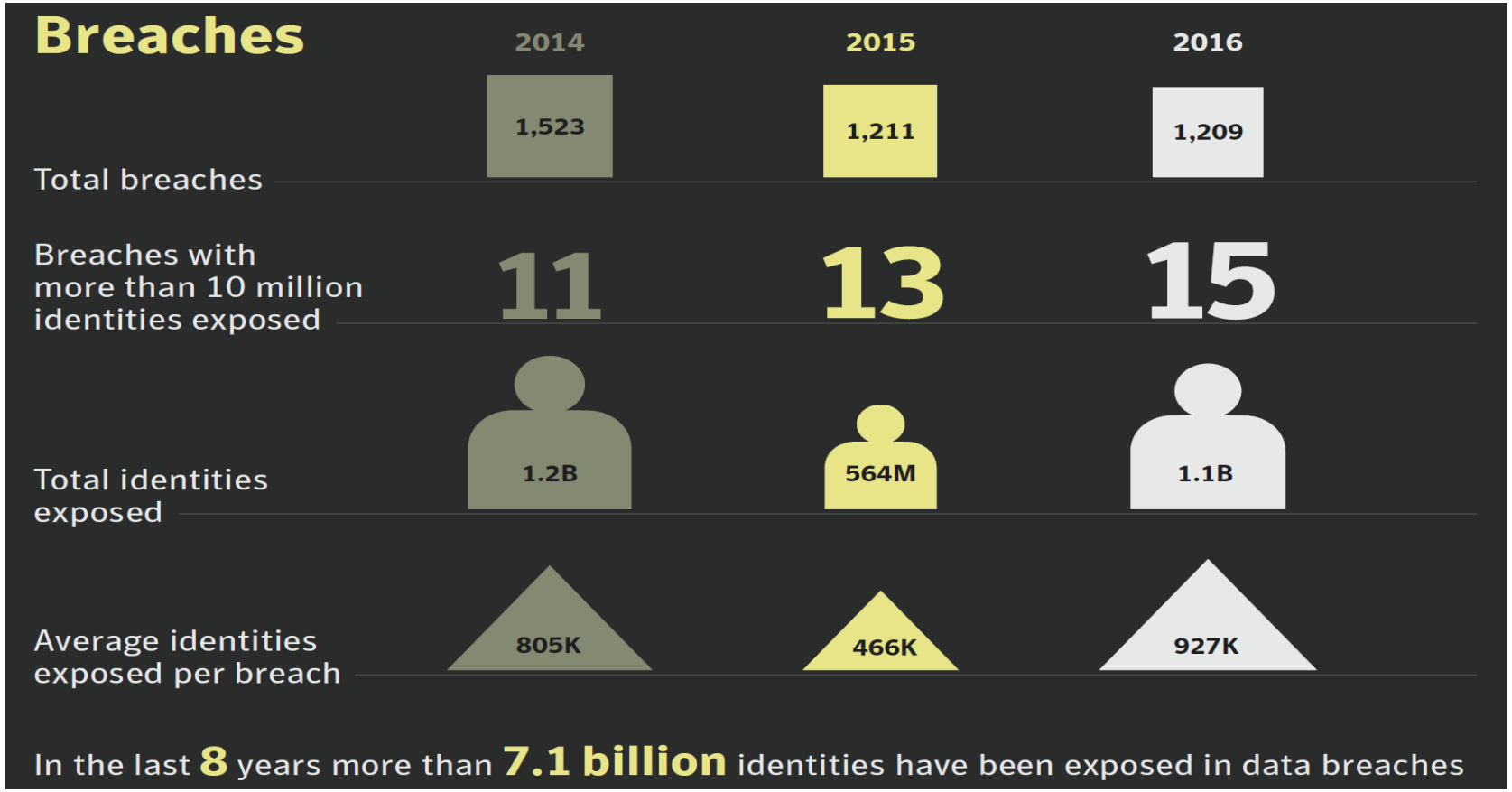
Takeaways

- **Sense of urgency** to address unsustainable trends and exploit rare economic development opportunity to create hundreds of thousands of middle class jobs
- Industry/government/academic coalition led by industry to address **"skills gap"** and talent pipeline
- Connect education directly to a job through a dual learn and earn **registered apprenticeship program (Because "Nothing Else Works")**
- Develop **skilled workforce** based on validated competencies and industry standard certifications
- Apprenticeships are good for business with **positive return on investment**

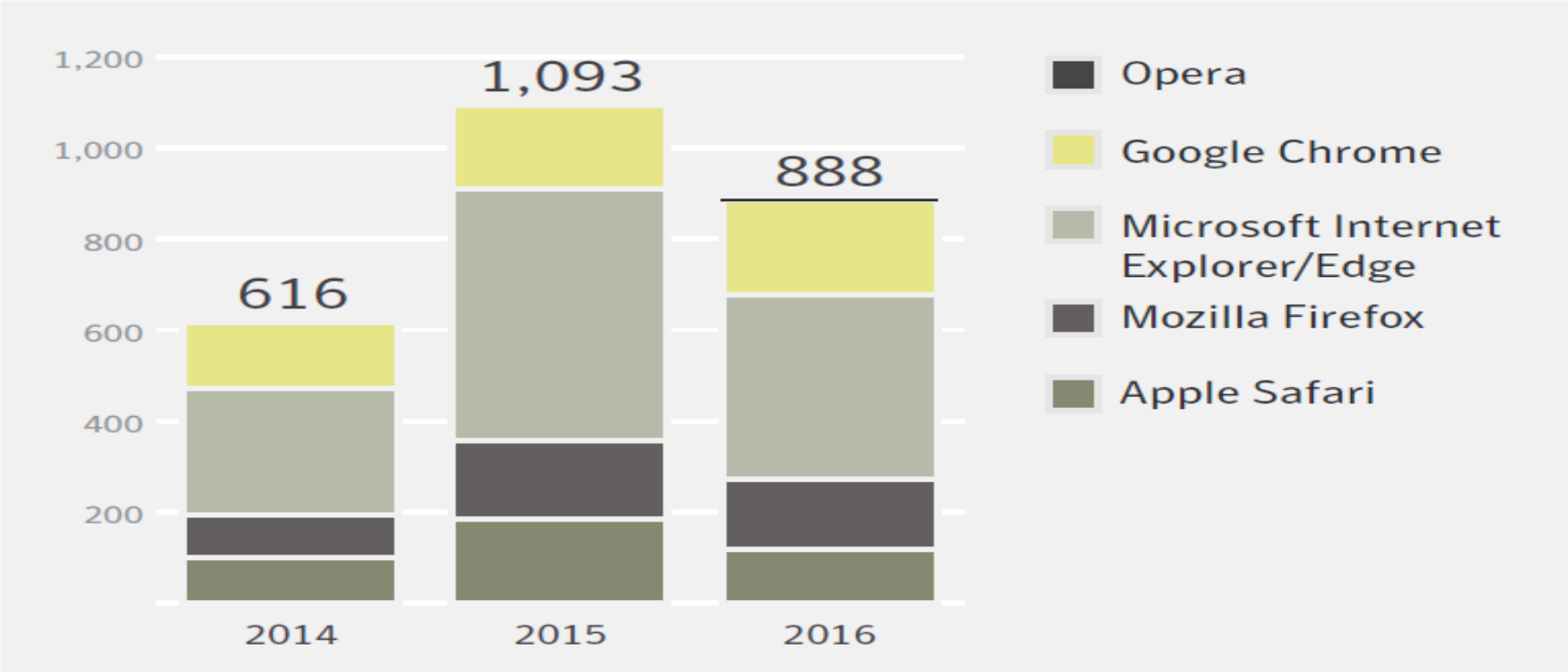
Why We Are Here

- Increasing number of cyber attacks against critical infrastructure
- 90% of attacks are successful by exploiting defects in software
- Software developers not trained to deliver software with fewer vulnerabilities
- 1.5 million cybersecurity jobs currently unfilled
- High youth unemployment and large number of under-employed people
- Student debt > 1.0 trillion
- Cost of status quo

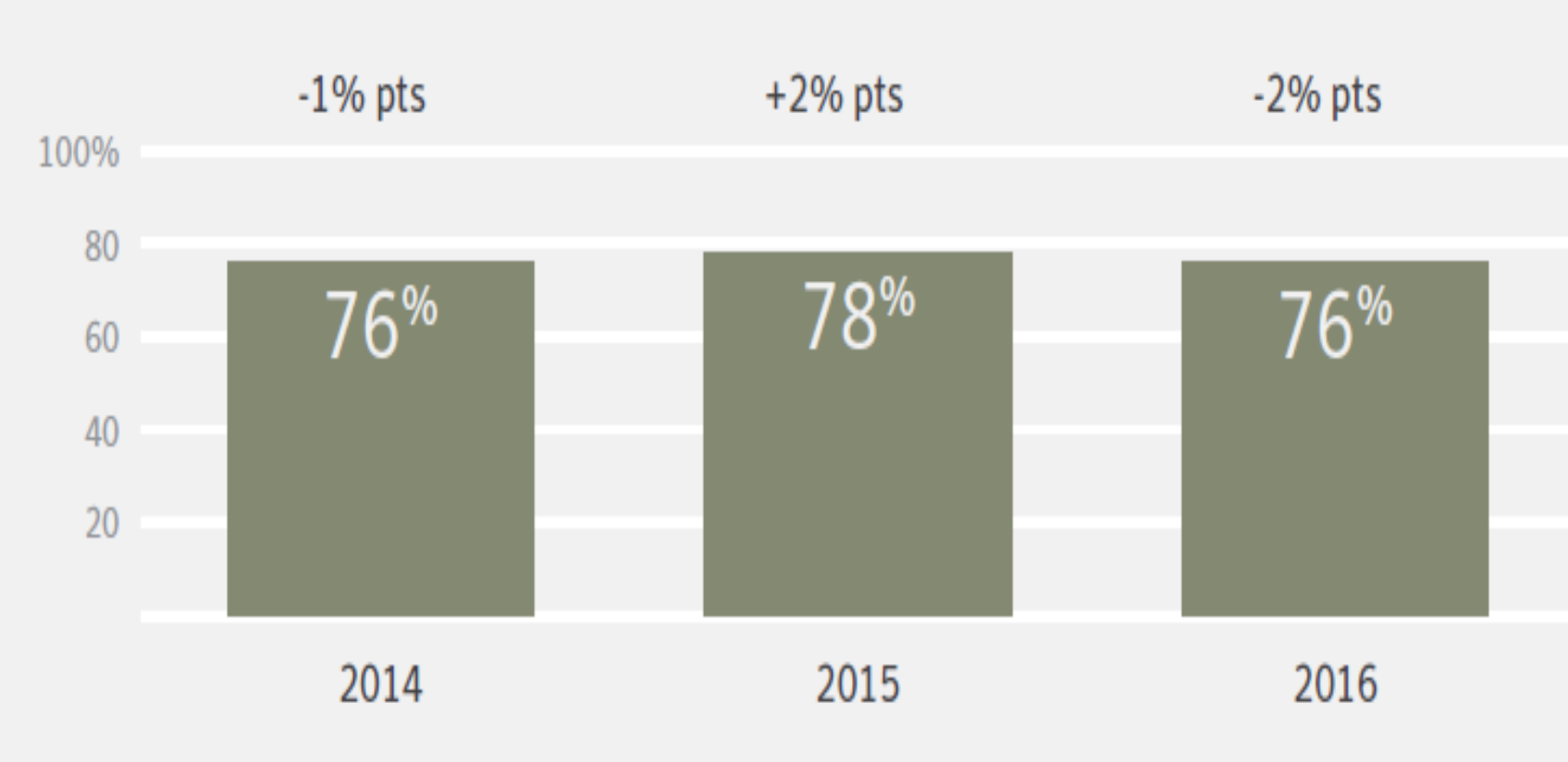
Personal Identity Breaches



Browser Vulnerabilities



Websites with Vulnerabilities



Patch and Pray - 1

Microsoft Patch Tuesday

On Tuesday, September 12, Microsoft released fixes for more than 80 security issues in multiple products, including Windows, Office, Microsoft .NET Framework, Flash, Internet Explorer, and Edge.

Patch and Pray - 2

Apache Struts Vulnerability Exploited in Equifax Breach

Equifax has acknowledged that the massive breach that exposed personal information of as many as 143 million people was due to a failure to apply a patch for a vulnerability in Apache Struts. A patch for the flaw was released on March 6, 2017. The Equifax breach occurred in "mid-May" 2017.

Patch and Pray - 3

Adobe Security Updates

Adobe has released updates to address security issues in Flash Player, ColdFusion, and RoboHelp for Windows. The Flash updates, available for Windows, Mac, Linux, and Chrome OS, address two critical memory corruption flaws. The ColdFusion update includes fixes for four flaws, and the RoboHelp update fixes two flaws

Patch and Pray - 4

Patches dominate the Top of the News this week.

Bill Murray speaks for many when he writes: "The cost to tolerate or remediate a design, recording, or coding error goes up exponentially with the time to its discovery. **There is something fundamentally wrong with an industry in which the toleration, indeed the institutionalization, of late discovery and remediation of error is as it is in ours."**

And John Pescatore offers a path toward fixing that fundamental flaw in the software industry, describing a future where larger buyers of software (government, for example, along with the Business Roundtable) set a much higher bar for application security testing at multiple stages of the development life cycle, both for custom software they develop and for every package they buy, with **substantial contractual penalties for vendors who fail**.

What is at Stake - 1

Some US States Are Going Back to Paper Ballots

In the wake of rising concerns about the security of electronic voting systems, several US states are returning to the use of paper ballots for their elections. Georgia will pilot a paper-ballot system in elections this fall.

FDA Approves Pacemaker Patch, Announces Recall of Abbott/St. Jude Medical Devices

The US Food and Drug Administration (FDA) has announced a recall of more than 450,000 pacemakers because they require a firmware update to address several security issues. The recall applies to several models of pacemakers manufactured by Abbott, formerly known as St. Jude Medical. Patients must visit their doctor's office where the update can be installed while the device is in backup mode. The flaws could be exploited to gain unauthorized access to vulnerable devices and issue commands to modify the pacemaker's settings and functionality.

What is at Stake - 2

Car Safety Vulnerability Lies in the Way CAN Handles Error Messages

A vulnerability in the Controller Area Network (CAN) that exists in most new automobiles could be exploited to shut down components of the car, including safety systems. Any component connected to the car's CAN bus could be affected. The issue is not one that can simply be patched because it lies in the CAN bus messaging protocol standard. Components that send too many error messages are disconnected from the CAN, so if attackers can spoof error messages to appear to be coming from a targeted component, that component could be shut off from the CAN.

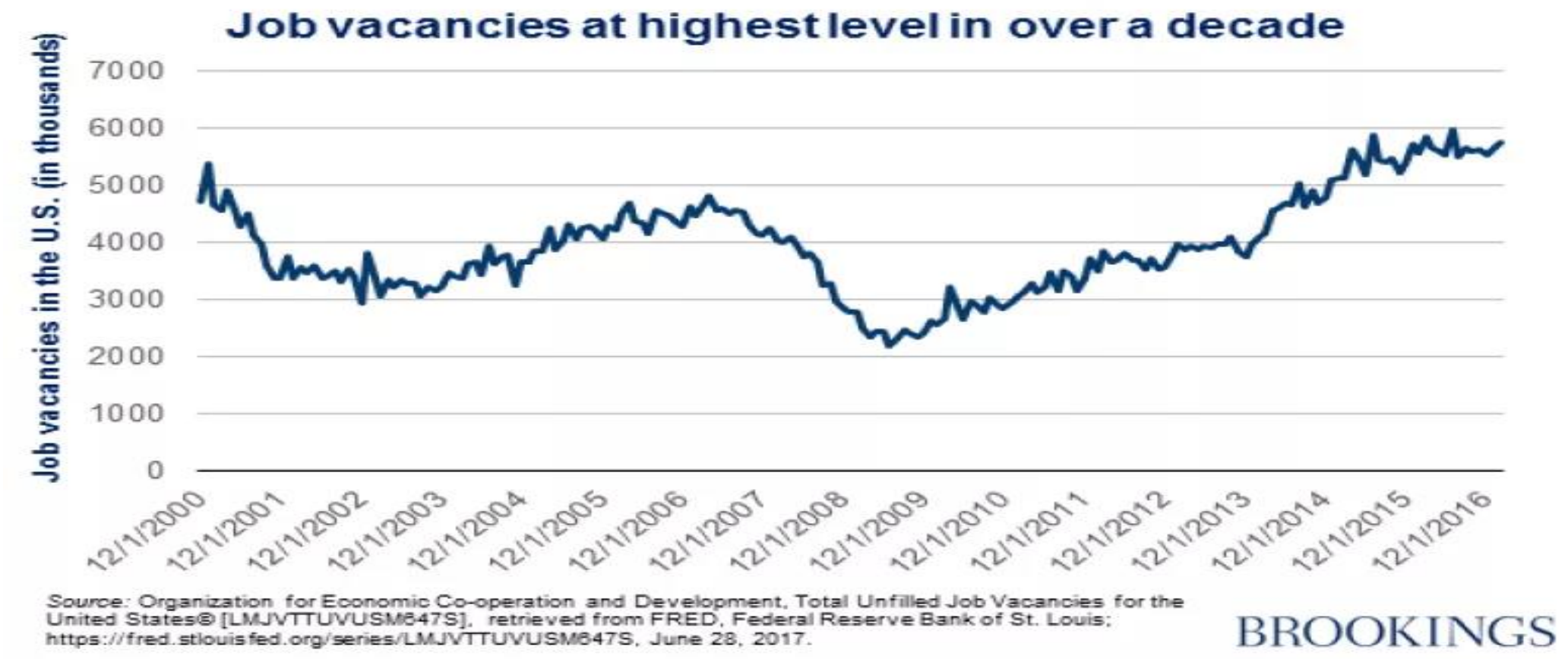
What is at Stake -3

National Infrastructure Advisory Council Report - A Pre 9-11 Moment

"There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber attack, [for the nation] to organize effectively and take bold action," said the US National Infrastructure Advisory Council report. The report lists 11 recommendations, including "establish separate, secure communications networks specifically designated for the most critical cyber networks; ... identify best-in-class scanning tools and assessment practices; ... [and] establish clear protocols to rapidly declassify cyber threat information."

What is at Stake - 4
IoT Risks

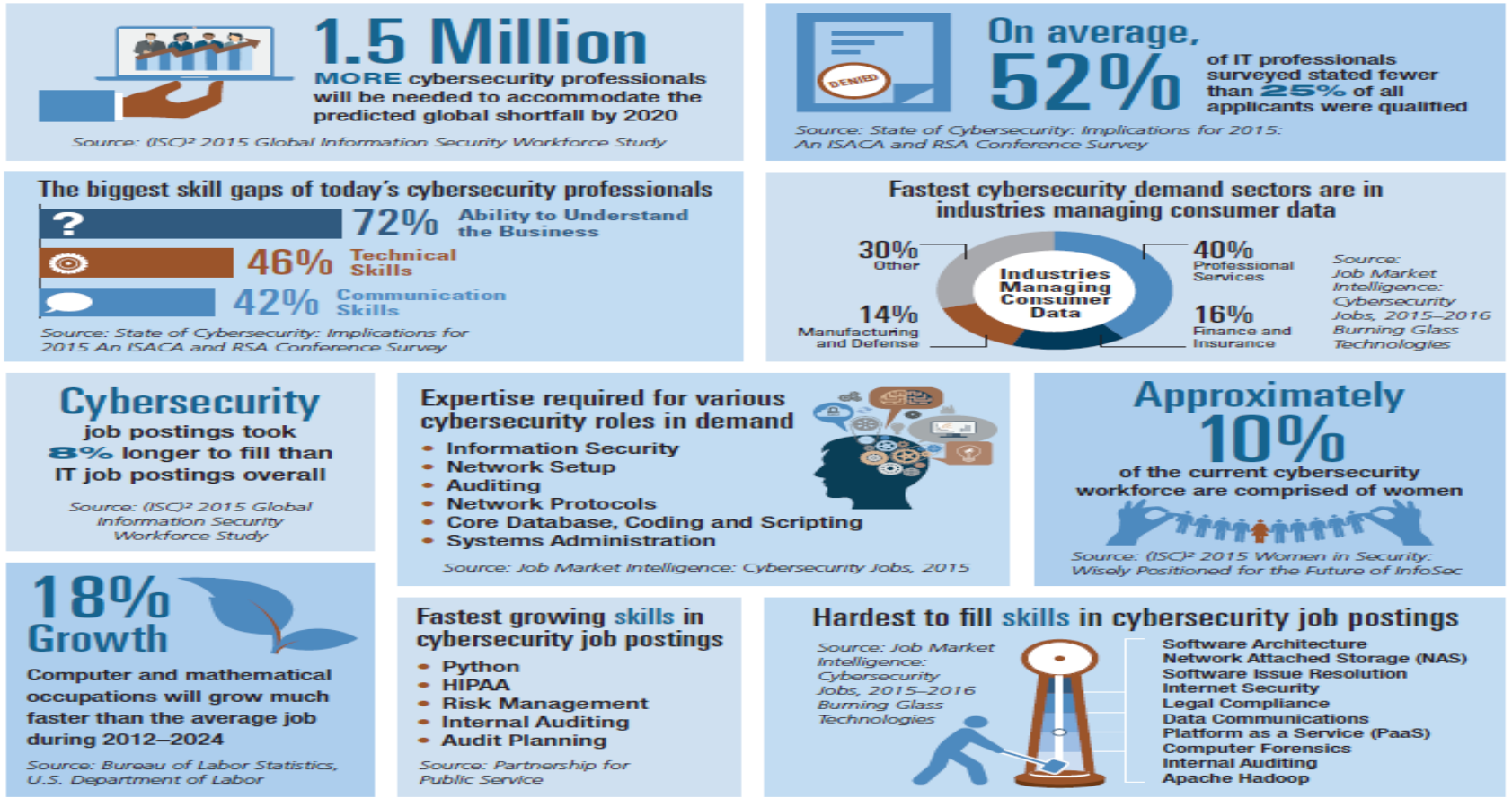
Total Number of Unfilled Jobs



Source: Organization for Economic Co-operation and Development, Total Unfilled Job Vacancies for the United States© [LMJVTTUVUSM647S], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/LMJVTTUVUSM647S, June 28, 2017.

BROOKINGS

Cybersecurity Skills Shortage



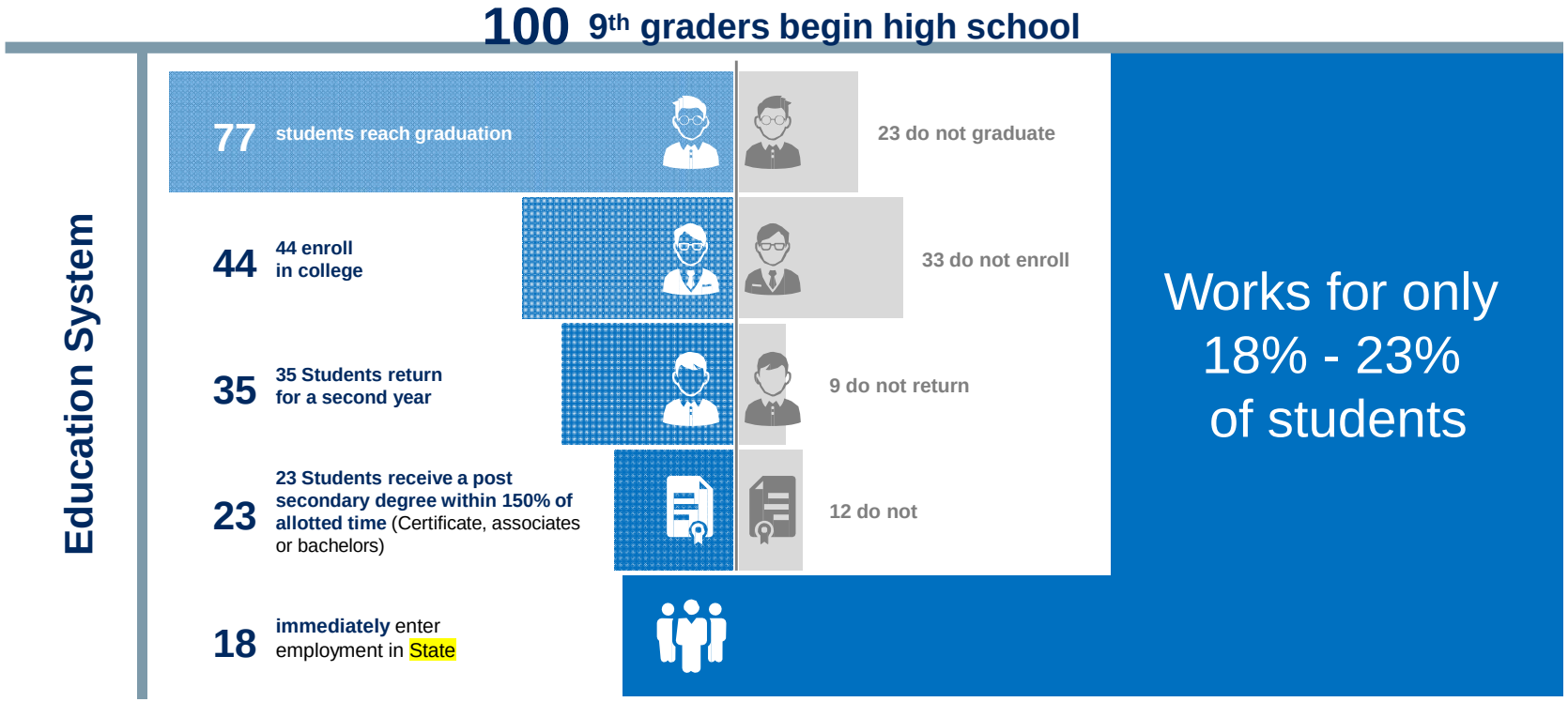
Cybersecurity: the Hottest New Major In College

Large numbers of US colleges have added undergraduate cybersecurity majors, cybersecurity concentrations to other majors, and master's degree programs in cybersecurity. Most colleges, however, do not know what to teach, and **many are teaching students only how to admire the cybersecurity problem, but not how to fix it.** Further, computer science graduates don't learn secure coding or other technical cybersecurity topics. None of the top ten undergraduate computer science and engineering programs at American universities (as ranked by the U.S. News & World Report) required its students to take a cybersecurity course in order to graduate.

Read more in:

- www.villagevoice.com: How Cybersecurity Became 2017's Hot New Major

Educational System's Challenge



The challenge: How do we prepare the talent needed by business to be globally competitive

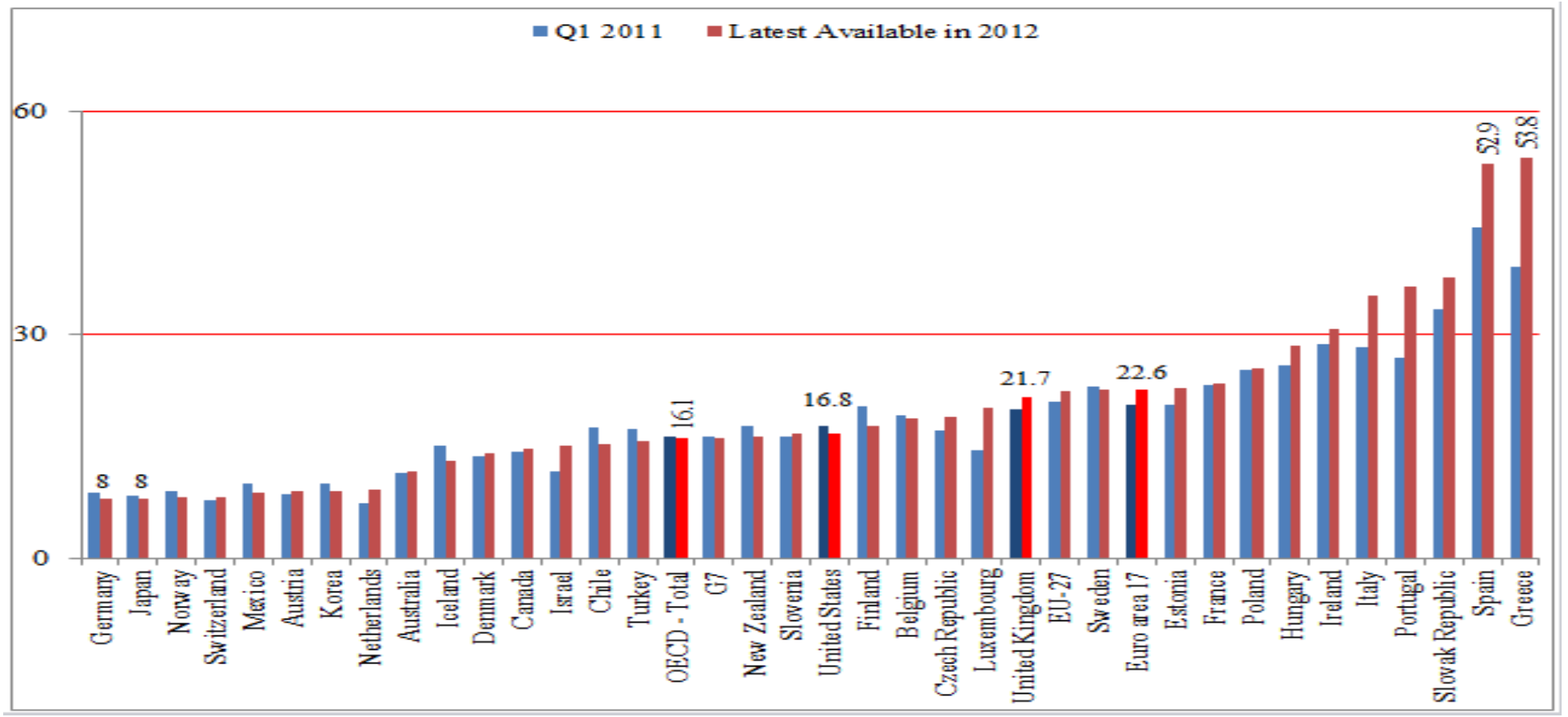
Cost of Status Quo

Item	Cost
Two-year and four-year college	$400 billion per year
Post-secondary workforce education and training	$600 billion per year
Skills gap	$160 billion per year
Time for new employees to reach full productivity	> Five months on average
Replacing an employee	Ranges from 6 to 24 months of the position's salary

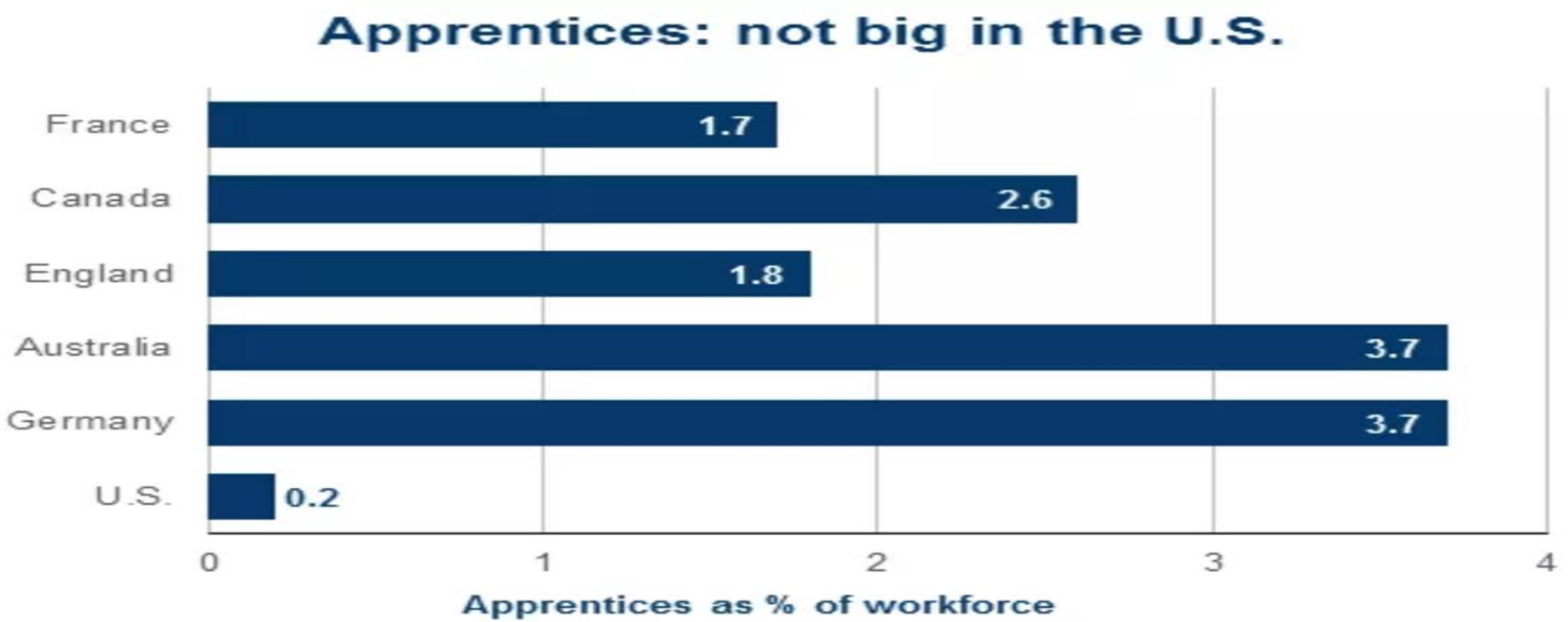
Source: Georgetown University Center on Education and the Workforce

Swiss Dual Track Vocational Education and Training Model

Youth Unemployment



Apprenticeships in the U.S.



Source: Robert Lerman, "Are Employers Providing Enough Training? Theory, Evidence and Policy Implications," prepared for National Academy of Sciences, 2015

BROOKINGS

US Department of Labor Initiative

ApprenticeshipUSA

- An exciting national renewal and reimagining of registered apprenticeship
- Learn, borrow and steal from Europe
- Expand in new, non-traditional industries and occupations
- $165 million in new funding for Registered Apprenticeship

DoL Registered Apprenticeship Requirement

5 Core Components of Registered Apprenticeship

Employer Involvement Is Integral	Employer is the foundation for the RA program and must be directly involved and provider of OJT
Structured On-the-Job Training with Mentoring	Minimum of 2,000 hours Structured and Supervised
Related Training and Instruction	**144 hours recommended per year** Parallel | Front-loaded | Segmented Options
Rewards for Skill Gains	Increases in skills brings about increases in earnings
National Occupational Credential	Nationally recognized credential showing job proficiency. Sponsor certifies individual is fully competent for career.

Employer-Led Collaborative Design

Why Apprenticeships?

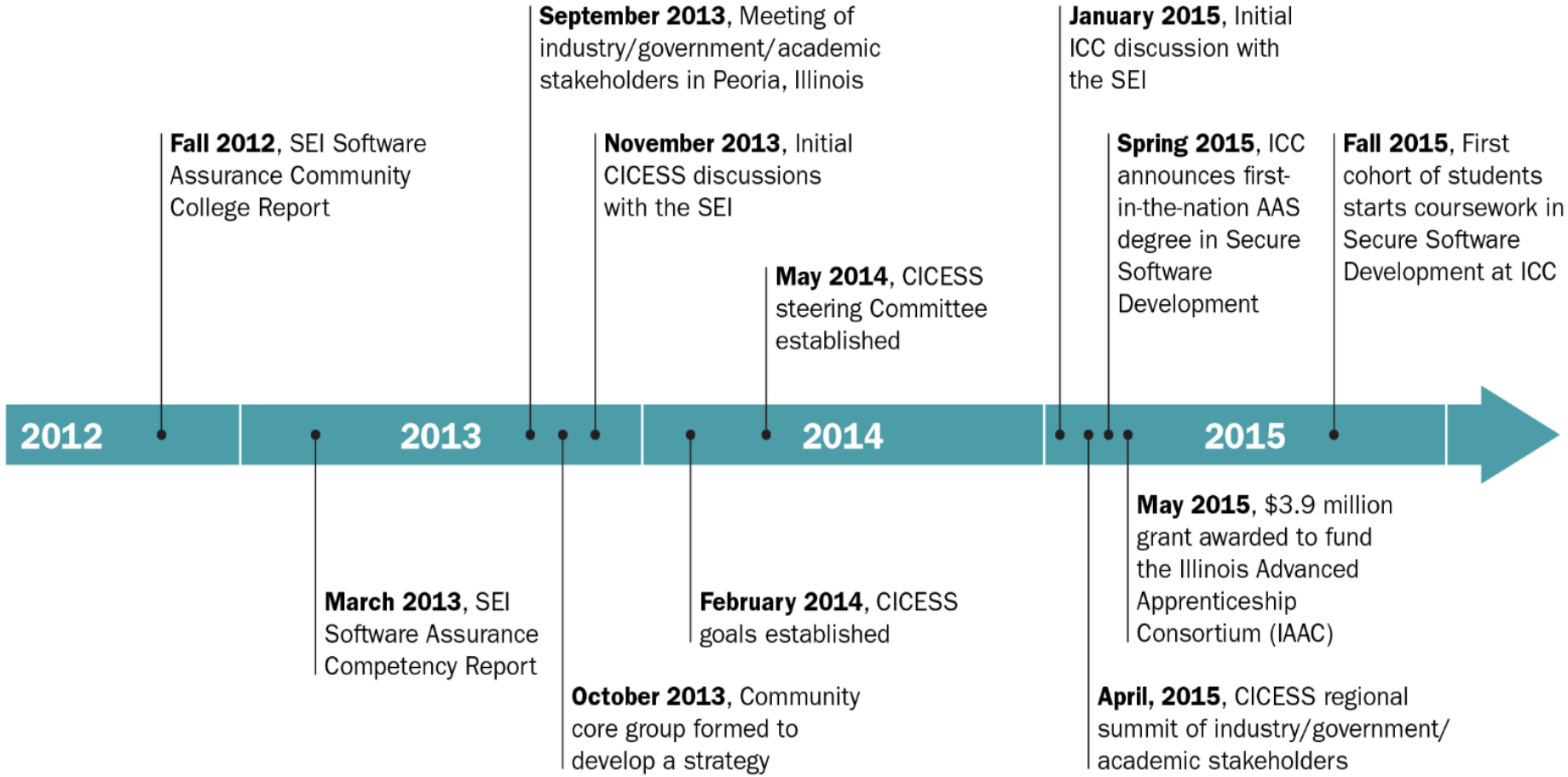
Because Nothing Else Works

CICESS

- Community Initiative Center of Excellence for Secure Software
- Solving Cybersecurity Skills Shortage With Apprenticeships and Certifications
- Launched successfully in Fall 2015, partnering with Illinois Central College and the Peoria Public Schools

A Unique Collaboration – Industry, Government, Academe

Timeline for the Community College and Industry Apprenticeship Program



CICESS Design – 1

- Standard academic curriculum leading to first-in-the-nation AAS Degree in Secure Software Development
- Berger Aptitude Test (B-Apt) for Computer Programming for entry to the apprenticeship program
- Standard apprenticeship curriculum based on Carnegie Mellon University Software Engineering Institute (CMU/SEI) process models
- Validate secure software development competencies – $(ISC)^2$ CSSLP, SEI PSP Developer certifications

CICESS Design – 2

- Alternating blocks of weeks of academic instruction and apprenticeship on-the-job training in the dual model
- Recurring and one-time-only fees from participating employers for ongoing program administration, apprenticeship curriculum development, and train-the-trainer materials
- Guidelines for minimum hourly wages for the apprentices with flexibility to meet varied human resources practices of participating employers

Apprenticeship Dual Model
Computer Programing (Secure Software)

2-3-year dual model "learn and earn" program

On the job training	Class room instruction
Employment contract executed between company and apprentice	Full time student AAS degree in Secure Software Development at local community college
Dual work study model with increasing hours under company supervision and mentorship as training progresses	Dual work study model with more classroom hours at the beginning
Standard apprenticeship topics defined by industry and aligned with Carnegie Mellon University / Software Engineering Institute	Curriculum created by Carnegie Mellon University and adopted to meet industry requirements

Practicum examination and standard industry certifications to validate competency

Secure Software Development AAS Degree

CS I: Programming in Java

CS II: Programming in Java

CS III: Advanced Programming in Java

Structured Query Language

Introduction to Relational Database

C# Programming

Mobile Application Programming

Introduction to Computer Security

Secure Coding

Introduction to Assured Software Engineering

Database Administration

Structured System Analysis

Two electives in computer programming, web, or networking, depending on employer needs

Students must also take 19 credit hours in general education courses.

Alignment with Federal Initiatives

- DHS Cybersecurity Workforce Framework
- NSA Centers of Academic Excellence
- NIST Cybersecurity Education
- DoL American Apprenticeship Initiative
- DoL Registered Apprenticeship standards

CICESS Value Proposition

- Augmentation of your current workforce development methods
- Ability to plan for and satisfy future needs for hard-to-fill secure software developers
- Ability to build a secure software talent pipeline that includes women and minorities who are trained, mentored, and certified
- A cost-effective solution to training and retaining new workers in secure software development
- High retention rates when apprentices become full-time employees

Takeaways/"ASKs"

- Act with a **sense of urgency** to address unsustainable trends and exploit rare economic development opportunity to create hundreds of thousands of middle class jobs
- Develop industry/government/academic coalition led by industry to address cybersecurity **"skills gap"** and talent pipeline
- Take immediate steps to connect education directly to a job through a dual learn and earn **registered apprenticeship program**
- In your community, develop **skilled workforce** based on validated competencies and industry standard certifications
- Stay on the message: Apprenticeships are good for business with **positive return on investment**

Contact

Girish Seshagiri

girish.seshagiri@ishpi.net

703 426-2790