Education Advisory Board | COE Forum

Multi-track Cybersecurity Pathways

Industry Futures Series

COE Forum

Executive Director

Chris Miller

Contributing Consultants

Lisa Geraci
Jess Jong
Lisa Qing

Practice Manager

Carla Hickman

Design Consultant

Stefanie Kuchta

LEGAL CAVEAT

The Advisory Board Company has made efforts to verify the accuracy of the information it provides to members. This report relies on data obtained from many sources, however, and The Advisory Board Company cannot guarantee the accuracy of the information provided or any analysis based thereon. In addition, The Advisory Board Company is not in the business of giving legal, medical, accounting, or other professional advice, and its reports should not be construed as professional advice. In particular, members should not rely on any legal commentary in this report as a basis for action, or assume that any tactics described herein would be permitted by applicable law or appropriate for a given member's situation. Members are advised to consult with appropriate professionals concerning legal, medical, tax, or accounting issues, before implementing any of these tactics. Neither The Advisory Board Company nor its officers, directors, trustees, employees and agents shall be liable for any claims, liabilities, or expenses relating to (a) any errors or omissions in this report, whether caused by The Advisory Board Company or any of its employees or agents, or sources or other third parties, (b) any recommendation or graded ranking by The Advisory Board Company, or (c) failure of member and its employees and agents to abide by the terms set forth herein.

The Advisory Board is a registered trademark of The Advisory Board Company in the United States and other countries. Members are not permitted to use this trademark, or any other Advisory Board trademark, product name, service name, trade name, and logo, without the prior written consent of The Advisory Board Company. All other trademarks, product names, service names, trade names, and logos used within these pages are the property of their respective holders. Use of other company trademarks, product names, service names, trade names and logos or images of the same does not necessarily constitute (a) an endorsement by such company of The Advisory Board Company and its products and services, or (b) an endorsement of the company or its products or services by The Advisory Board Company. The Advisory Board Company is not affiliated with any such company.

IMPORTANT: Please read the following.

The Advisory Board Company has prepared this report for the exclusive use of its members. Each member acknowledges and agrees that this report and the information contained herein (collectively, the "Report") are confidential and proprietary to The Advisory Board Company. By accepting delivery of this Report, each member agrees to abide by the terms as stated herein, including the following:

1. The Advisory Board Company owns all right, title and interest in and to this Report. Except as stated herein, no right, license, permission or interest of any kind in this Report is intended to be given, transferred to or acquired by a member. Each member is authorized to use this Report only to the extent expressly authorized herein.

2. Each member shall not sell, license, or republish this Report. Each member shall not disseminate or permit the use of, and shall take reasonable precautions to prevent such dissemination or use of, this Report by (a) any of its employees and agents (except as stated below), or (b) any third party.

3. Each member may make this Report available solely to those of its employees and agents who (a) are registered for the workshop or membership program of which this Report is a part, (b) require access to this Report in order to learn from the information described herein, and (c) agree not to disclose this Report to other employees or agents or any third party. Each member shall use, and shall ensure that its employees and agents use, this Report for its internal use only. Each member may make a limited number of copies, solely as adequate for use by its employees and agents in accordance with the terms herein.

4. Each member shall not remove from this Report any confidential markings, copyright notices, and other similar indicia herein.

5. Each member is responsible for any breach of its obligations as stated herein by any of its employees or agents.

6. If a member is unwilling to abide by any of the foregoing obligations, then such member shall promptly return this Report and all copies thereof to The Advisory Board Company.

Table of Contents

Cybersecurity's Skills Gap 4

A White-Hot Specialty in a Red-Hot Field 4

Cybersecurity Demand Growing Faster Than IT Sector Overall 4

Corporations Staffing Up to Address Cybercrime and Privacy Concerns 5

Every Industry Taking Note 6

Cybersecurity Supply Still Lags Demand 7

Too Few Cybersecurity Graduates 7

Why Aren't We Producing Enough Cybersecurity Professionals? 7

Emerging Career Ladders 8

Charting the Cybersecurity Career Path 8

Leveling the Playing Field 8

Bellwether Federal Employers Redefine Cybersecurity's Must-Have Skills 8

Core Foundational Content, Mix-and-Match Optional Units 9

Optional Knowledge Units Offer Tremendous Potential for Bundling, Stackability 10

Designing a Cybersecurity Curriculum 11

Program Options for All Budgets 11

Large and Small Programs Find Success Regionally, Nationally 11

Critical Infrastructure Sectors 12

Programs Append Field-Specific Security and Privacy Courses 12

Just-in-Time Executive Education 13

Programs Prioritize Customer Service 13

Online-Only Cybersecurity Stacks 14

Cross-Listed Cyber Programs Grow Portfolio at a Lower Cost 14

Getting Big Isn't Cheap 16

Scalable Virtual Security Labs Require Costly Hardware 16

Assessing the Opportunity for Your Institution 17

Regional Cybersecurity Needs 17

Key Locations for Cybersecurity Present Opportunities for Regional and Online Programs 17

Opportunities for Cross-Listing 18

Offer Non-tech Electives Alongside Technical Coursework 18

About the COE Forum 19

Serving University COE Administrators 19

Research and Insights 19

Performance Technologies 19

Cybersecurity's Skills Gap

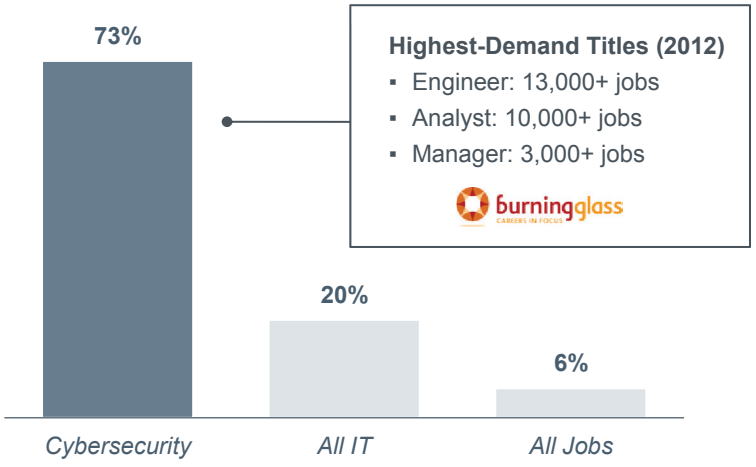
A White-Hot Specialty in a Red-Hot Field

Cybersecurity Demand Growing Faster Than IT Sector Overall

As we continue to integrate technology into daily life and companies become reliant on the cloud, growth in demand for IT professionals is expected. While IT roles are predictably growing at a fast clip, the growth of cybersecurity positions is staggering. Cybersecurity positions grew by 73% between 2007 and 2012, compared to 20% in IT, and 6% across all sectors.

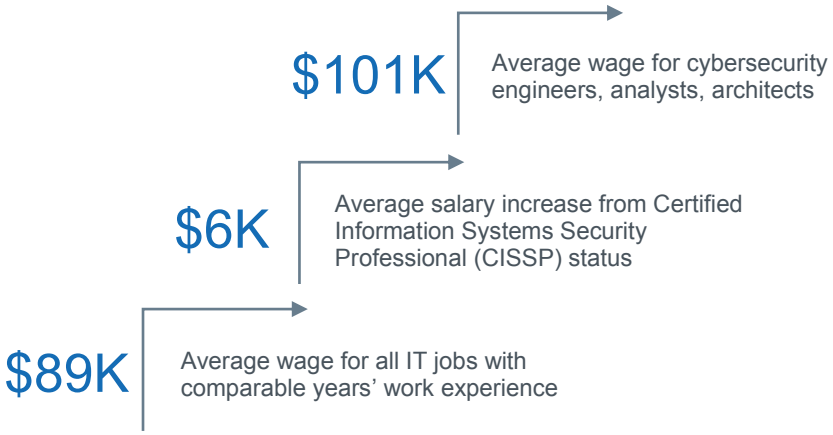
Exploding Employer Demand[1]

Increase in Online Job Postings, 2007-2012



In addition to higher demand for cybersecurity skills, professionals in cybersecurity positions earn more than most IT employees. Even a short certification (e.g., CISSP), increases salary potential by $6,000.

A Growing Wage Premium[2]



1) "Initial Findings on Cyber Security Jobs," Burning Glass Technologies, February 2013.
2) Burning Glass Labor/Insight.

©2014 The Advisory Board Company • 29363_D

Corporations Staffing Up to Address Cybercrime and Privacy Concerns

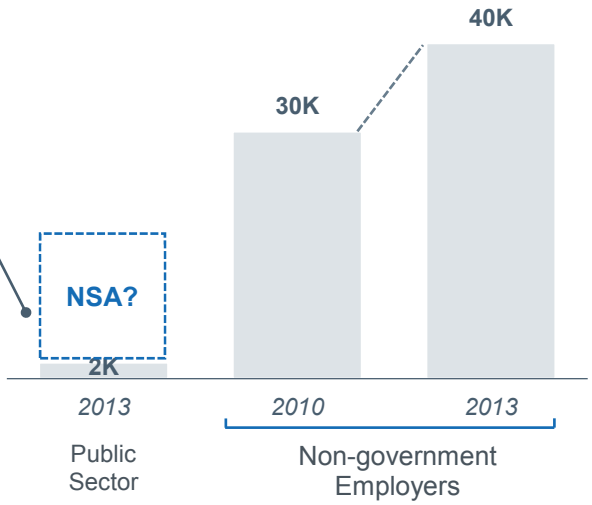
The demand for cybersecurity skills is growing as both sides—the good (government organizations, private companies) and the bad (organized crime syndicates)—staff up in response to one another. Cybercrime is no longer the result of lone hackers. In fact, the cost of global cybercrime is equal to that of the drug trade.

Cybersecurity concerns also extend beyond the public sector.[3] The general public's awareness of security concerns in the commercial sector increased after the data breach at Target in fall 2013 and the Heartbleed Bug in spring 2014. However, companies started to build defense teams and strategies for their networks years before these events. Between 2010 and 2013, the demand for cybersecurity professionals among non-governmental employers rose 30%, and researchers anticipate continued growth in the next several years.[4]

From National Security to Private Sector[5, 6]

Cybersecurity Job Postings, 2010 vs. 2013

Few public-sector cybersecurity positions appear in online job postings due to discreet hiring practices. At present, intelligence organizations are thought to employ hundreds of thousands of employees.



From Hackers to Syndicates

108K

Number of U.S. cybersecurity incidents reported, 2011

$100B

Estimated cost of global cybercrime fraud from Russian Business Network

3) Andrea Shalal-Esa, "Scores of U.S. Firms Keep Quiet About Cyber Attacks," Reuters, June 2012.
4) Rashid, Fahmida Y, "Cyber Security Market to Reach $120B by 2017," *SC Magazine*, July 2012.
5) Frank Umbach, "Cyber Threats Are Growing in Size, Volume, and Sophistication," *World Review*, May 2003.
6) Burning Glass Labor/Insight.

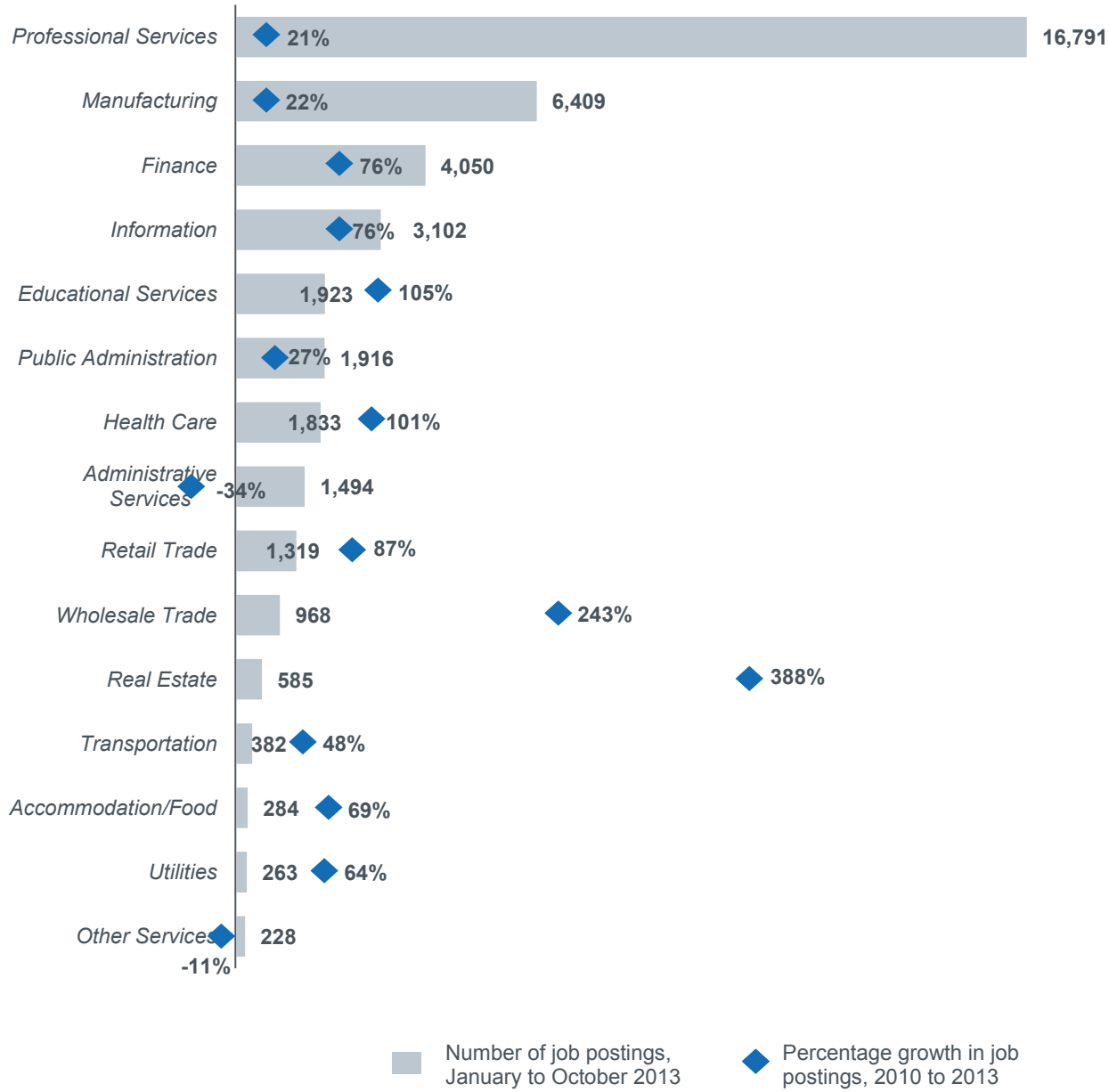
Every Industry Taking Note

As public and private companies sit on an increasingly large amount of data, demand for cybersecurity professionals is growing in all sectors. Predictably, the health care, finance, and information industries reported significant growth in demand for cybersecurity professionals; less expected industries like real estate and wholesale trade also experienced significant gains. Top titles across industries include:

- Security Engineer
- Security Analyst
- Information Security Analyst
- Network Security Engineer

Broad Growth in Cybersecurity Job Postings Across Sectors[7]

Cybersecurity Job Postings by Industry, 2010-2013



7) Burning Glass Labor/Insight.

Cybersecurity Supply Still Lags Demand

Too Few Cybersecurity Graduates

Why Aren't We Producing Enough Cybersecurity Professionals?

Despite high salaries and employer demand across industries, employers struggle to find qualified candidates for cybersecurity positions. Most cybersecurity programs are off-limits to students who lack a professional background in IT, while existing cybersecurity professionals frequently change careers due to a lack of advancement opportunities. These barriers threaten to exacerbate cybersecurity's workforce shortage, though opportunities abound for educational programs that appeal to entry-level workers or career changers without a technical background.

Barriers to Pursuing Cybersecurity Jobs[8,9,10]

Hard to Fill Despite High Pay

35%

Rate at which employers are more likely to re-post a cybersecurity job, versus another IT job, due to a lack of qualified candidates

Curriculum Misalignment	**Overcredentialing** Master's programs proliferate, despite the fact that most employers prefer a bachelor's degree. 23% *Percent of cybersecurity jobs that required or preferred a graduate degree in 2012*	**Lack of On-Ramps** Few programs offer foundational courses to retrain non-IT workers, limiting the pool of qualified applicants. 43% *Percent of cybersecurity workers who first became interested the field after starting their careers*
Unclear Career Value Proposition	**Low Awareness** Lack of exposure to security careers during K-12 education produces college-bound students unaware of cybersecurity. 82% *Percent of Millennials to whom no high school teacher or counselor had mentioned cybersecurity careers*	**Unclear Career Path** Weakly defined opportunities for professional growth compel cybersecurity professionals to change careers. #1 *Rank of "greater growth opportunity" among top reasons cybersecurity workers change jobs*

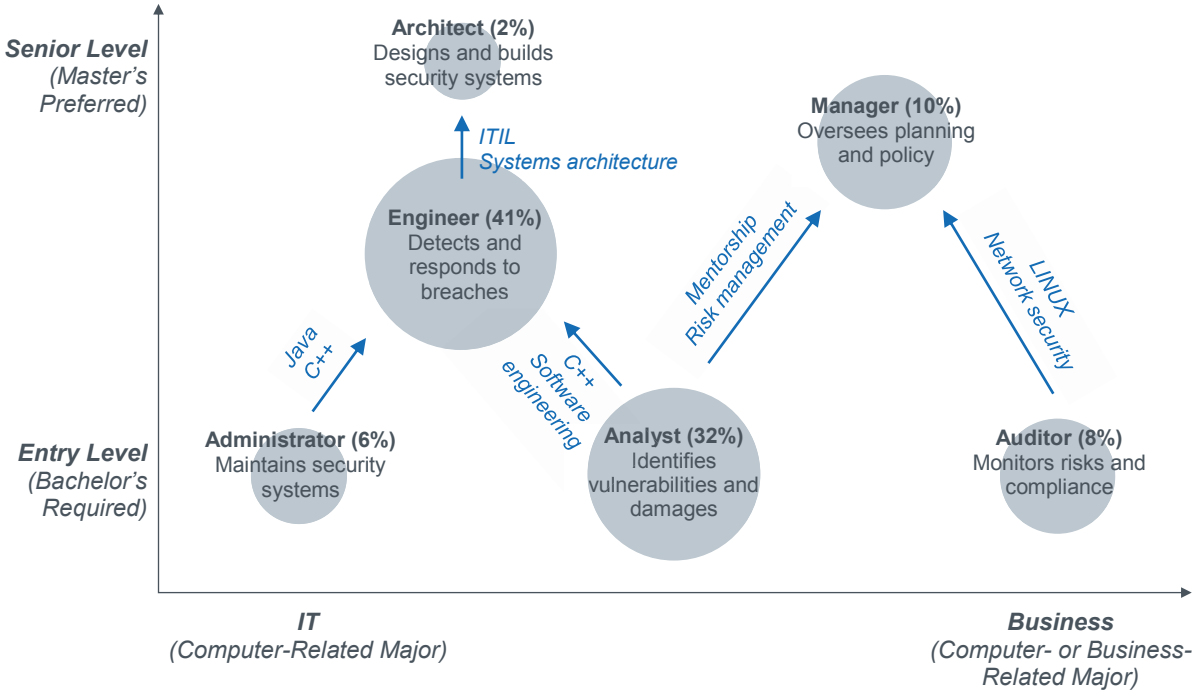
8) "Preparing Millennials to Lead in Cyberspace," Raytheon, October 2013.
9) "Cyber Security Census," Semper Secure, August 2013.
10) Burning Glass Labor/Insight.

Emerging Career Ladders

Charting the Cybersecurity Career Path

Cybersecurity is still a relatively new field, with new roles, titles, and positions emerging every year. The graphic below illustrates the skills that separate career starters from mid-level employees, and mid-level employees from senior-level employees across a technical spectrum. The percentages represent the share of job postings each type of role represents. The number of jobs that require master's degrees remains small and emphasizes the need for entry-level training.

Map of Cybersecurity Roles by Education and Experience Level[11,12]



Leveling the Playing Field

Bellwether Federal Employers Redefine Cybersecurity's Must-Have Skills

The current designation for program excellence in cybersecurity is the Center of Academic Excellence (CAE) in Information Assurance and Cyber Defense certification, sponsored by the National Security Agency (NSA) and Department of Homeland Security (DHS). However, the proliferation of CAE designations (now held by 181 institutions) and a lack of standardization across institutions has corroded its original reputation.

To recalibrate programs against the new standards, all institutions must reapply for the CAE status by December 2014. The new application requires cybersecurity programs map their curriculum to the 64 course topics and learning outcomes outlined by the NSA and DHS.[13]

11) "Cybersecurity Roles and Job Titles," The George Washington University Department of Computer Science, http://www.cs.gwu.edu/academics/graduate_programs/master/cybersecurity/cybersecurity-jobs.

12) Burning Glass Labor/Insight.

13) "National Centers of Academic Excellence in Information Assurance/Cyber Defense: New Academic Requirements," National Security Agency and Department of Homeland Security, June 2013.

Centers of Academic Excellence in Information Assurance and Cyber Defense

Distinctive in 2007
"We were the only school in the area with Center of Excellence status. It really helped with our enrollments."

Cybersecurity Program Director, Regional Public Institution

Common by 2012
"There are so many schools with the designation, it became more of a 'Center of Adequacy.'"

Faculty Leader, Large Public Research University

Reapplication in 2014

"The framework makes the requirements easier to update as the discipline evolves and allows for differentiation among schools."

CAE Team. 2013

- 181 institutions earned CAE status (including 33 community colleges)
- Wide variation in program formats and learning objectives

- NSA and DHS define 64 discrete knowledge units that mandate topics and learning outcomes
- Universities must reapply for Center of Excellence Status by December 2014

Core Foundational Content, Mix-and-Match Optional Units

In a 75-page recertification document, the NSA and DHS identify the 10 knowledge units a student must possess to earn an associate's degree, an additional 5 units to earn a bachelor's degree, and 49 optional knowledge units. The assignment of core knowledge units provides a solid program development framework, while optional knowledge units provide opportunities for degree specializations and certificates.

Optional knowledge units may be bundled into dozens of concentrations, certificates, and contract trainings. Even if the NSA and DHS once again confer the CAE designation to hundreds of colleges and universities, each designee can stake their claim to a niche subset of cybersecurity education (e.g., mobile security, digital forensics).

NSA-DHS Information Assurance/Cyber Defense Knowledge Units[14,15]

Core Knowledge Units (15)

Two-Year Programs
- Data Analysis
- Introductory Programming
- Cyber Defense & Cyber Threats
- Fundamental Security Design
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Ethics, and Compliance
- System Administration

+

Four-Year Programs
- Databases
- Network Defense, Technology, and Protocols
- Operating Systems Concepts
- Probability and Statistics
- Programming

14) Partial list of 64 knowledge units. Full list available at http://www.cisse.info/pdf/2014/2014%20CAE%20Knowledge%20Units.pdf.

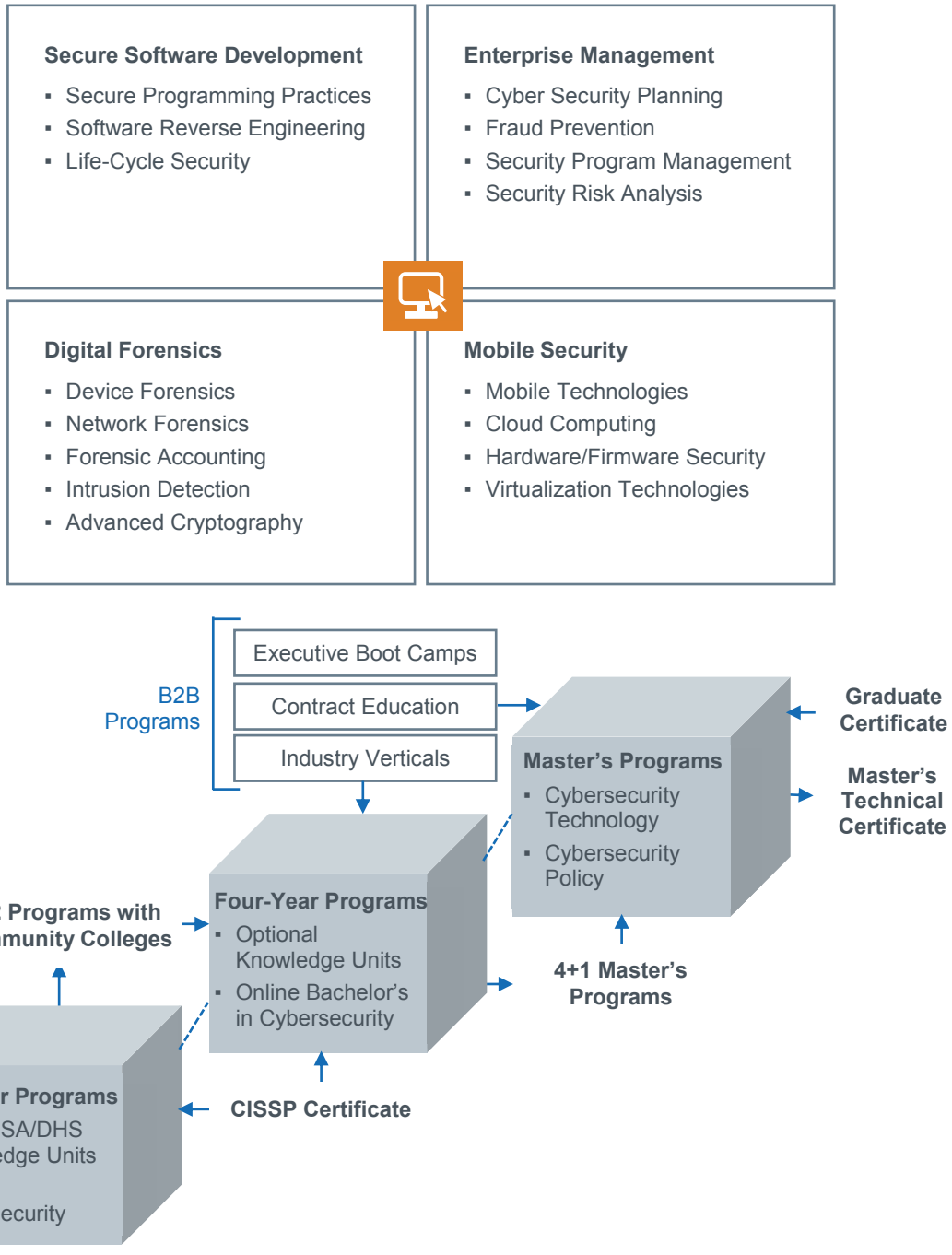
15) "National Centers of Academic Excellence in Information Assurance/Cyber Defense: New Academic Requirements," National Security Agency and Department of Homeland Security, June 2013.

Optional Knowledge Units Offer Tremendous Potential for Bundling, Stackability

The new CAE guidelines create numerous possibilities for stackability and competency-based learning. Administrators can develop two-year programs that stack on top of associate's degrees, as well as 4+1 master's programs that combine core knowledge units with specializations. Bundled core and optional units also provide opportunities for B2B programs for both technical and non-technical workers.

Knowledge unit-based programs lend themselves well to competency-based learning formats, as students with some background in cybersecurity, either through courses or professional experience, can test out of courses by demonstrating expertise in that topic. This "test-out" ability allows students to enter programs at different stages and increases the number of potential applicants.

Flexibility of Optional Knowledge Units

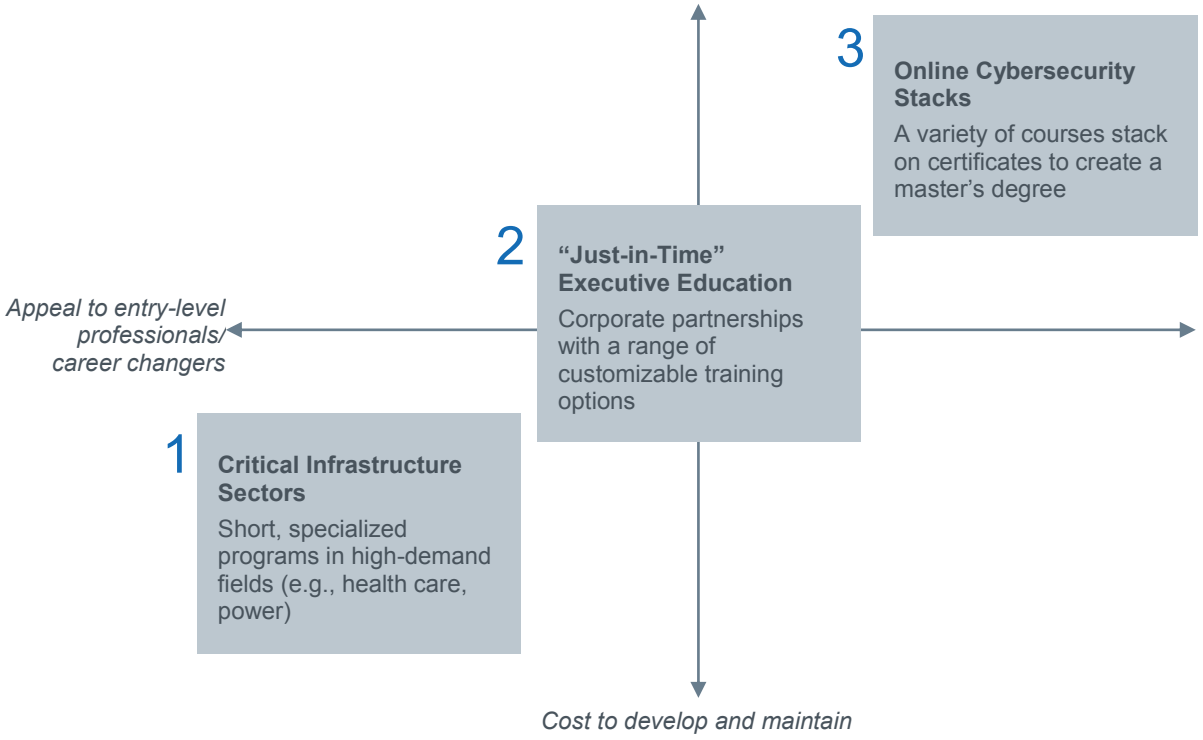


Designing a Cybersecurity Curriculum

Program Options for All Budgets

Large and Small Programs Find Success Regionally, Nationally

Cybersecurity programs are accessible to nearly all COE units, regardless of an institution's budget or existing infrastructure in computer science or information technology. Program options range from low-cost niche certificates to highly profitable program suites with multiple tracks and concentrations.



Programs Append Field-Specific Security and Privacy Courses

Industry-specific cybersecurity programs require the least amount of resources to develop and maintain. These short programs combine two to three cybersecurity courses with coursework from existing professional programs (e.g., health informatics, finance). Although these programs are among the easiest to create, their target audience is limited. A Cybersecurity for Finance Professionals certificate, for example, is limited to people in the financial sector.

Safeguarding Patient Information at Boston University[16]

BU's Medical Information Security & Privacy

Format

- Graduate certificate
- 4 courses; hybrid

Courses

- Database Security
- Enterprise Information Security
- Health Informatics
- Electronic Health Records

Jobs

- Health Information Security Specialist
- Chief Healthcare Information Officer

Protecting the "Smart Grid" at Worcester Polytechnic Institute[17]

WPI's Cybersecurity for Today's Power Industry

Format

- Graduate certificate
- 6 courses; online asynchronous

Courses

- Software Security
- Operations Risk Management
- Intrusion Detection
- Industry Case Studies

Jobs

- SCADA Network Security Specialist
- Cyber Threat Intelligence Analyst

16) "Medical Information Security & Privacy Graduate Certificate," Boston University Metropolitan College, http://www.bu.edu/met/programs/graduate/medical-information-security-privacy-certificate/.

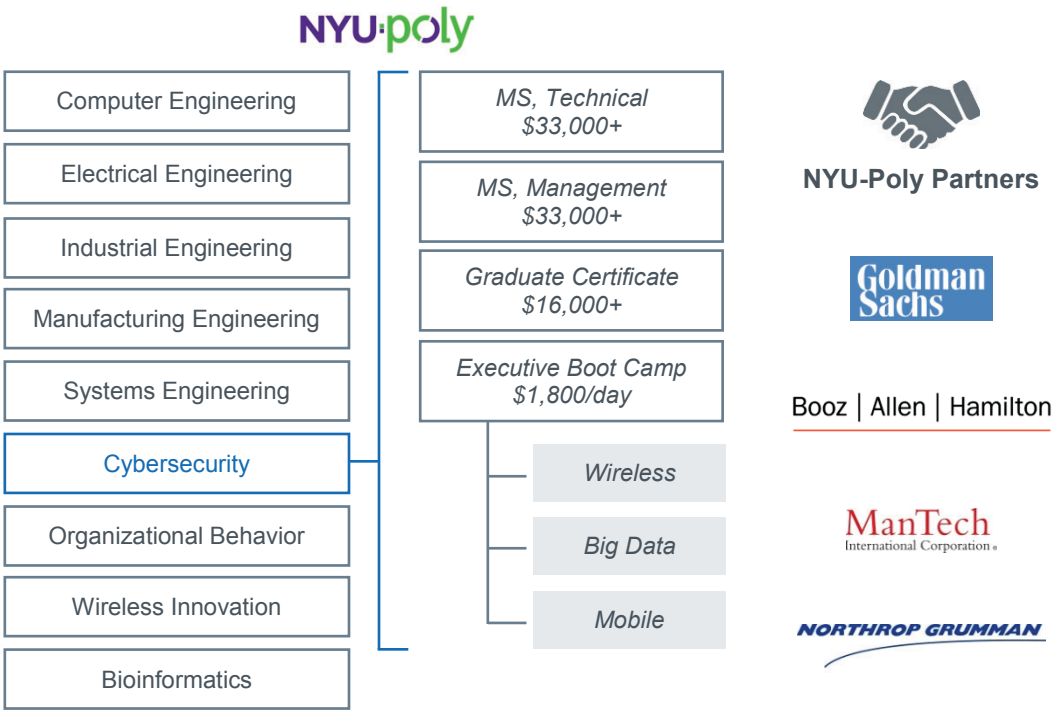
17) "Cyber Security Education with a Power Industry Focus," Worcester Polytechnic Institute, http://cpe.wpi.edu/cybersecurity.html.

Just-in-Time Executive Education

Programs Prioritize Customer Service

Corporate partnerships offer high potential for enrollments but demand significant resources to serve customers and customize course content. NYU-Poly, the engineering school of New York University, offers stackable corporate partnerships in a variety of fields. Clients may enroll current or aspiring cybersecurity employees in a variety of programs that suit a range of training needs and budgets, from one-day boot camps to master's degrees.

Program Clusters Target Mid-Career Professionals[18]



A commitment to customer service supplements NYU-Poly's suite of courses and degree programs. Discounts to loyal clients, a dedicated relationship manager assigned to each institution, and customized content and delivery incentivize clients to sponsor more employees.

"Enterprise Partner" Privileges

Cohort Discounts
Tuition reductions for 12+ employees who enroll together

Corporate Concierge
Helps employees navigate current online courses, map future ones

Customizable Programs
Mixing general training and company-specific initiatives

18) "Enterprise Learning," NYU-Poly, http://engineering.nyu.edu/enterprise-learning.

Online-Only Cybersecurity Stacks

Cross-Listed Cyber Programs Grow Portfolio at a Lower Cost

The University of Maryland University College (UMUC) maintains one of the largest cybersecurity programs in the United States, with tracks and concentrations that appeal to companies and individuals from technical and non-technical backgrounds. UMUC offers a variety of undergraduate and graduate programs; the latter consists of 12 master's and certificate offerings in which students can elect a technical focus or a policy focus. Despite the number of graduate-level offerings at UMUC, a large portion of courses are cross-listed among programs, reducing the cost of creating and maintaining new tracks or focuses.

"Versioning" Core Cybersecurity Content[19]

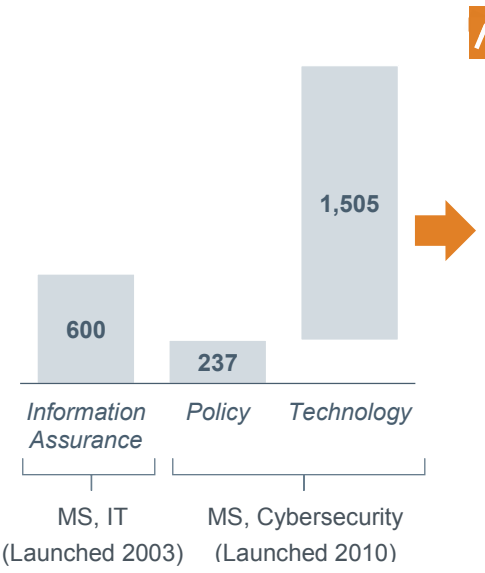
	Technical	*Policy*
Master's	▪ MS, Cybersecurity ▪ MS, Information Assurance ▪ MS, Digital Forensics	▪ MS, Cybersecurity Policy ▪ MS, Homeland Security Specialization
Graduate Certificate	▪ Cybersecurity Technology ▪ Information Assurance ▪ Digital Forensics	▪ Foundations of Cybersecurity ▪ Cybersecurity Policy ▪ Homeland Security Management

UMUC

As their graduate portfolio grew, administrators at UMUC experienced no cannibalization of existing programs. Enrollment in the university's original program in information assurance remained stable, and the new policy and technology tracks sufficiently appealed to new markets.

Steady Program Growth Since 2003

UMUC Graduate Enrollments, 2013



…And Only Growing From Here

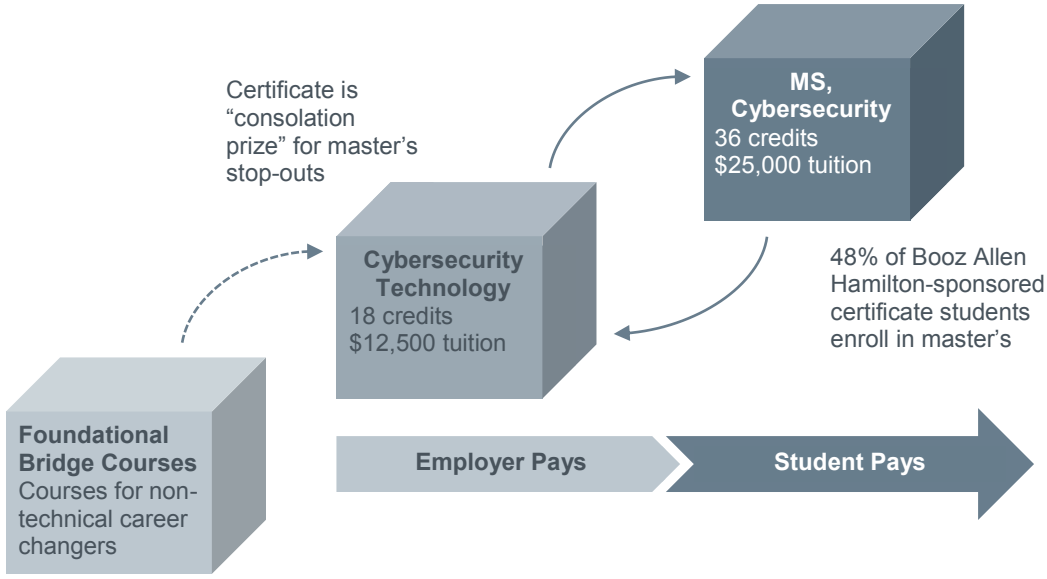
Program directors at UMUC are brainstorming ways to grow enrollments even larger. Ideas include:

- **Competency-Based Programs** that allow experienced IT professionals to move quickly through familiar content
- **Foundational Bridge Courses** that reduce barriers to entry among aspiring cybersecurity professionals with no technical background

19) Master's Degrees in Cyber Security," University of Maryland University College, http://www.umuc.edu/cybersecurity/academics/masters-degrees.cfm; "Graduate Certificates in Cyber Security," University of Maryland University College, http://www.umuc.edu/cybersecurity/academics/certificates.cfm.

Cybersecurity certificates prove especially valuable for the UMUC portfolio, as employers are more likely to sponsor a certificate than a degree. Students who complete certificates are then more likely to enroll in a full degree program since their employer already paid half of the tuition. Alternatively, for students who enroll directly in the master's program, the certificate acts as a "consolation prize" for students who drop out or stop out.

Stackability Reduces Students' Cost and Risk



Create On-Ramps for Non-technical Professionals

Foundational bridge courses can offer an additional "on-ramps" for non-technical career changers who lack the prerequisites to enter graduate-level programs. Introductory information technology courses may also improve retention rates for students without a technical background. Typical courses include:

- Calculus
- Intro to Programming (Java, C++)
- Data Structures
- Computer Architecture
- Networking Fundamentals

Getting Big Isn't Cheap

Scalable Virtual Security Labs Require Costly Hardware

Even though UMUC cross-lists courses across programs, the infrastructure to support additional students remains costly. Administrators consider their virtual security lab an integral part of the program and a major selling point for students, as it gives them hands-on experience and access to the software and hardware used in the workplace. However, the virtual lab must accommodate any student who seeks access. At most times, the number of active users is fairly low, but usage can rise to hundreds of concurrent sessions during finals periods.

$1 Million+ for 300 Concurrent Sessions in Teaching Tools[20]

- **Experiential Learning**
  Live intrusion response decision-making, without asking student to configure own software or damaging actual network
- **Explore O/S Features**
  Students use full functionality of market-standard NMap and Nessus security tools
- **24/7 Availability for Hundreds of Concurrent Sessions**
  Labs must be "always on" for asynchronous work, but scalable during peak weeks

Hardware Costs Alone: $1.5M

Virtual Security Lab Hardware Requirements (Partial)

Industry partners and affiliated community colleges can share the cost of virtual lab equipment

- **Storage Array** $540,000
- **Switch** $12,000
- **Secure Port** $60,000
- **Servers** $560,000
- **Routers** $25,000
- **IPB Image** $50,000

20) Joon Son, Chinedum Irrechukwu, and Patrick Fitzgibbons, "A Comparison of Virtual Lab Solutions for Online Cyber Security Education," *Communications of the IIMA* (Vol 12): 81-101.

Assessing the Opportunity for Your Institution

Regional Cybersecurity Needs

Key Locations for Cybersecurity Present Opportunities for Regional and Online Programs

Industry-specific cybersecurity needs vary by location. The categories below list the locations with the greatest demand for cybersecurity skills in that industry. Demand for cybersecurity professionals remains high throughout the United States, with demand surging even in unexpected markets like Bismarck, Louisville, and Virginia Beach.*

Professional Services
Washington, DC
Chicago
New York
Atlanta
Boston

Manufacturing
Washington, DC
Baltimore
Dallas
San Jose
New York

Financial
New York
Dallas
Minneapolis
Chicago
Washington, DC

Information
Washington, DC
New York
Seattle
San Jose
Los Angeles

Educational Services
Washington, DC
New York
Los Angeles
Boston
Baltimore

Public Administration
Washington, DC
Chicago
Baltimore
San Diego
Virginia Beach

Health Care
Washington, DC
New York
Chicago
Rochester (MN)
Nashville

Administrative Services
Chicago
Washington, DC
New York
Dallas
Seattle

Retail Trade
Seattle
Chicago
Atlanta
San Francisco
Phoenix

Wholesale Trade
Chicago
Atlanta
Providence
Portland
San Jose

Real Estate
St. Louis
Los Angeles
Washington, DC
New York
Dallas

Transportation
Chicago
New York
Atlanta
Washington, DC
Seattle

Accommodation and Food Services
Las Vegas
New York
Seattle
Louisville
Phoenix

Utilities
Los Angeles
Dallas
Baltimore
Bismarck
Minneapolis

*Demand also includes the cities' surrounding metropolitan areas

Opportunities for Cross-Listing

Offer Non-tech Electives Alongside Technical Coursework

Although employers unsurprisingly seek employees with a strong technical background, the nature of cybercrime requires that cybersecurity professionals possess an understanding of the financial and legal implications of the field. In addition to computer science coursework, consider cross-listing courses in business, finance, criminal justice, mathematics, and law.

Top Computer Science and Specialized Skills in Demand for Cybersecurity Professionals[21]

Bachelor's or Master's Degree Preferred/Required, Nationwide, May 2013-April 2014

Computer Science Skills
Firewalls (15,714)
Network Security (11,802)
LINUX (10,070)
UNIX (9,701)
CISA (9,221)
Cyrptography (7,436)
Cisco (5,932)
Transmission Control Protocol/IP (5,729)
System and Network Configuration (5,372)
Scanners (5,297)
JAVA (4,601)
Oracle (4,343)
SQL (4,342)
Network Engineering (4,008)
Disaster Recovery Planning (3,990)
PERL (3,951)
Virtual Private Networking (3,900)
System Administration (3,666)
Systems Engineering (3,599)

Business Skills
Risk Assessment (4,246)
Risk Management (3,637)
Business Process (3,621)
Business Development (1,392)
Business Administration (1,385)
Technical Writing/Editing (3,271)
Process Improvement (1,342)

Finance Skills
Internal Auditing (3,767)
Accounting (3,376)
Asset Protection (2,321)
Audit Planning (2,051)
Audit Experience (1,521)

Other
Forensics (2,595)
Mathematics (2,300)
Telecommunications (2,294)
Legal Compliance (1,847)

21) Burning Glass Labor/Insight.

About the COE Forum

Serving University COE Administrators

Our Parent Firm: The Advisory Board Company

Founded in 1979 to serve hospitals and health systems, The Advisory Board Company is one of the nation's largest research and consulting firms serving nonprofit, mission-driven organizations. With a staff of over 2,500 worldwide, including 1,150 in Washington, D.C., we serve executives at about 3,800 member organizations in more than two dozen countries, publishing 50 major studies and 15,400 customized research briefs yearly on progressive management practices.

Our Work in Higher Education: EAB

Encouraged by leaders of academic medical centers that our model and experience serving nonprofit institutions might prove valuable to colleges and universities, the Advisory Board launched our higher education practice in 2007. We are honored to report over 700 college and university executives now belong to one of our EAB memberships.

Research and Insights

Business Affairs Forum

Research and support for college and university chief business officers on improving administrative efficiency and lowering costs.

Academic Affairs Forum

Strategy advice and research for provosts, deans, and other academic leaders on elevating performance in teaching, research, and academic governance.

Student Affairs Forum

Research for student affairs executives on innovative practices for improving student engagement and perfecting the student experience.

COE Forum

Breakthrough-practice research and market intelligence to help universities develop and grow continuing, professional, and online education programs.

Advancement Forum

Breakthrough-practice research and data analytics to help advancement professionals maximize philanthropic giving and support institutional goals.

Community College Forum

Strategy advice and research for community college presidents on improving college finances and campus management, as well as partnering with four-year institutions.

Performance Technologies

University Spend Collaborative

Business intelligence, price comparison database, and consulting to assist chief procurement officers in reducing spend on purchased goods and services.

Student Success Collaborative

Combines technology, research, and predictive analytics to help institutions positively inflect outcomes with at-risk and off-path students.