THINKING AND TALKING ABOUT

CYBERSECURITY

CAREER AWARENESS
CONTENTS

CHAPTERS PAGE
1: FILLING OUT THE CYBERSECURITY WORKFORCE 4
2: TEACHING MORE THAN JUST TECHNICAL SKILLS 7
3: MANY DIMENSIONS TO SUCCESS IN CYBERSECURITY 10
4: EMPATHY AND PROBLEM-SOLVING 13
5: FINDING KIDS WHO CAN AND WANT TO DO THE JOB 15
6: CYBER AND STEM ARE A GOOD FIT 19
7: WIDENING THE LENS 22
8: HOW WE WOULD LIKE TO HELP 25

ERIC IVERSEN, Ph.D.
Vice President, Learning and Communications
Start Engineering

Eric Iversen has worked in education for over 25 years, as a teacher, publisher, administrator, and author. At Start Engineering, he develops and produces learning content about educational and career pathways in STEM careers, with a focus on engineering and cybersecurity. Products delivered to market include field guidebooks, student workbooks, teacher's guides, curricula, and an award-winning blog about STEM issues and trends. He is in charge of digital marketing, communications, and social media; he speaks publicly about STEM education topics at live events and on broadcast media; and he conducts independent and collaborative projects on STEM learning and career activities in formal and informal K-12 learning environments. He has launched and led varied learning enterprises, both online and in-person. These programs have ranged from cross-platform, Internet-based learning to classroom-style education and outreach activities. He has held senior leadership positions with extensive management and strategy responsibilities at non-profit organizations involved in education and technology fields. He also taught college-level English for seven years, including both literature and writing courses.
NEW FROM Start Engineering:

CYBER CAREER AWARENESS PROGRAM

Perfect for classrooms, camps, competitions, and outreach!

Easy-to-use, flexible, and cost-effective.
Over 20 hours of lessons and workbook activities!

Helps educators — even with no training in the field —
guide students to understanding why cybersecurity matters to
them and how it could be a great career option.

Download sample pages and check out a video about the program at
https://start-engineering.com/cybersecurity-cybercap

To order, go to https://start-engineering.com/shop

For questions, email Bob Black at bblack@start-engineering.com or call 202-841-1524.
Two numbers underscore the urgency of efforts to grow the pool of students willing to consider a career in cybersecurity.

3.5 million – The number of unfilled cybersecurity jobs projected around the world by 2022. As an absolute figure, that represents a bounty of jobs for cybersecurity workforce entrants to consider.

1.8 – The ratio of cybersecurity workers to job openings now, compared to 3.7 workers to 1 job opening in the workforce overall. As a relative figure, that means there is about twice as much “opportunity” in cybersecurity as in the overall job market.

Up-to-date, granular information about the state of the cybersecurity job market is available at Cyberseek. By sector, by location, by almost any variable you like, analysis
and discussion of the cybersecurity workforce should always include reference to this 
resource.

From the perspective of job-seekers, these are heady times to be developing skills and 
looking for work in cybersecurity. From the perspective of hiring managers – and the 
society at large that relies on safe, reliable internet access and services – these are unset-
tling times.

Workforce shortages of this magnitude in a field as critical to our well-being as cyberse-
curity should motivate all of us to do whatever we can to attract more, and more differ-
ent kinds, of good candidates to the field. To catalyze and direct constructive solutions 
across all these domains, the National Initiative for Cybersecurity Education, or NICE, 
rolled out a new strategic plan in October 2020. It addresses education, training, and 
workforce development topics, all directed at expanding the size and capabilities of 
the country’s cybersecurity enterprise.

Short-term solutions run from recruiting more women and veterans to on-the-job train-
ing to machine-learning-based technology innovations. Long-term solutions mean 
education and outreach, to younger and more diverse audiences, with new methods 
and more appealing messages. We need to be offering the students already interested in 
the field more imaginative, multi-disciplinary programs and pedagogies. And we need to 
be telling a story about opportunities and pathways in cybersecurity that persuades girls,
under-represented groups, and non-technical kids that the field could be right for them. National Cybersecurity Career Awareness Week (NCCAW) is a flagship effort aimed at mobilizing resources to build interest in cybersecurity careers. An annual November event headed up by the National Initiative for Cybersecurity Education, it encompasses local, regional, and national efforts to build awareness about career opportunities in the field and the vital needs it serves for the country.

A strategic pillar of NCCAW is consistent messaging to students about the appeal and benefits of a cybersecurity career. A core messaging point states, “Cybersecurity has something for everyone,” and stresses the need for a diversity of skills, interests, and backgrounds among cybersecurity professionals. Indeed, the new NICE strategic plan folds this message into “Goal #1: Promote the Discovery of Cybersecurity Careers and Multiple Pathways.”

A look at the current cybersecurity workforce highlights the need to reach a larger population of students.

- At 26 percent minority, **cybersecurity workers are more diverse** than the overall workforce rate of 21 percent. However, minority workers skew lower in rank and pay than their white peers, notwithstanding education and experience levels.

- At 20 percent female, **the workforce offers up a large gender gap**, with women also getting paid less and promoted less, even though they bring more degree credentials to their jobs than men do.

Not for nothing has the **Girl Scouts’ recently launched badge in cybersecurity** attracted widespread attention and comment, among many other outreach efforts oriented towards girls. Making an appeal to students beyond the traditional populations of computer-oriented, mostly male students already primed to consider work in the field is key to building the kind of diverse cybersecurity workforce we need.
The future cybersecurity workforce will need to be larger and more diverse, to be sure. It will also need a wider variety of cognitive skills and attributes. Technical training is likely to be the simplest feature of the workforce to lock down. Indeed, a May 2018 panel of industry leaders identified “insatiable problem-solving skills,” the ability to work on teams, and fearlessness in the face of failure as paramount, over and above computer-based skills. And recent research efforts identify critical workforce attributes as, “the requirement for systemic thinkers, team players, a love for continued learning, strong communication ability, a sense of civic duty, and a blend of technical and social skill.” For a full, up-to-date, and sophisticated examination of cybersecurity workforce challenges, read the New America Foundation report on the topic.

To engage students who fit within this broad spectrum of cybersecurity workforce needs will require more substantive, nuanced ways of talking about the field. It must go beyond the common approach of focusing on hardware, networks, and operating systems. It will take integration of cybersecurity content across all the many different disciplines that work in the field can actually touch.

This focus on the cross-cutting cybersecurity dimensions at work in highly disparate fields is another point of emphasis for NCCAW messaging. Cybersecurity careers are
noted to offer great “job flexibility,” serving as “a launching pad for jobs in business, design, intelligence, defense, medicine, law, government, and much more.” Indeed, any field that relies on the internet to develop or deliver products and services – which means nearly every career pathway imaginable – will be only more open to candidates who bring cybersecurity capabilities with them. What students should understand is that cybersecurity can be almost anyone’s angle of approach to a rewarding, interesting career in almost any field that interests them.

So students should be hearing that cybersecurity can be a great field for those with the interest and skills and motivation to succeed. As we work and communicate with students to start them on a cybersecurity pathway, we should also have in mind the educational endpoint we would like them to reach. That is, we should have an idea of the learning a strong candidate for success in cybersecurity would need to absorb.
In words that a professor of English or history might use, John McCumber, Director of Cybersecurity Advocacy for North America at (ISC)², lays out the case for breadth, imagination, and the long view of things to infuse the education we would give those whom we charge with developing solutions for cybersecurity challenges:

“Not everything can be solved with an algorithm…. People need to build up their knowledge. Philosophy, art, the ability to understand the sweep and impact of history. Technology changes, but the problems mankind has to deal with pretty much remain the same.”

These sentiments are consistent with what many cybersecurity leaders say in print and at meetings on the topic of what makes for success in cybersecurity. Technical chops, to be sure; but more than that goes into developing students’ abilities and preparing them for success in cybersecurity careers.

Establishing the learning profile of potentially successful cybersecurity hires matters a lot. Looking to the fewer than 200,000 students who graduate each year with degrees in computer science or engineering will make only a small dent in the 3.5 million jobs projected to need filling.

Moreover, if John McCumber is right, these students are not the only, let alone best, prospects for these jobs. In a report from the Center for Strategic and International Studies, employers in large numbers report computer science graduates routinely lack basic knowledge and skills needed to step into cybersecurity jobs. Significant on-the-job training is required to ground them in areas like computer architecture, data science, cryptography, networking, and secure coding principles.
MANY DIMENSIONS TO SUCCESS IN CYBERSECURITY

So, how can we know a strong candidate for cybersecurity success when we see one? If a technical degree is not a reliable indicator, what attributes do help identify someone who can step into a cybersecurity job, contribute to a team, and build a future in the field?

As a starting point, prospective cybersecurity professionals should bring business savvy to their areas of technical specialization. Cybersecurity is increasingly seen as an organization-wide requirement, and all employees need to apply security awareness to execution of their responsibilities. By the same token, cybersecurity professionals need to understand the larger business environment in which they work. “We want well-rounded professionals who understand a broad range of cybersecurity disciplines and who also understand the business side,” says Paige Adams, Group Chief Information Security Officer at Zurich Insurance.

Indeed, the cross-pollination of knowledge required to mesh cybersecurity and business operations can help to start reframing our understanding of what a “cybersecurity” job really is. One tech recruiting company surveyed cybersecurity companies in seven ma-
jor high-tech hubs to find out what areas were in highest demand. The largest number of open positions fell into these four areas:

- Software engineering, 41 percent
- Sales, 22 percent
- Marketing, 11 percent
- Operations, 10 percent

Clearly, technical skills matter a lot. But companies providing cybersecurity products and services need help in many other areas to make their businesses work. Duo Security, for example, has reported that about 85 percent of their hires do not have a formal background in information security. Their clients – including Facebook, Paramount Pictures, Toyota, and Yelp – do not mind.

At Duo and other companies, many of these hires without formal training can be easily imagined as working on the “business” rather than the “technical” side of cybersecurity. Such businesses put cybersecurity-knowledgeable people to work engaging new and current clients, assessing business opportunities, plotting strategies, and so on. But even among technical staff, formal training is not necessarily in their background. A 2016 survey of 56,000 developers from around the world found that 69 percent of them were fully or partly self-taught.
Cybersecurity jobs also extend to operational needs quite different from business development, strategy, and communications. Securing systems from attack, for example, requires defenses of both a digital and analog nature, if you will. Not only must systems be protected from hostile incursions via networks and hacked user profiles, but the buildings and physical surroundings in which they operate need robust safety systems, as well. Protecting the servers and machinery through which valuable data travel can involve everything from building design and security to protocols governing access and assessing human factors for risk.

Indeed, these “attack surfaces” can open systems up to existential risk. In perhaps the most notable such instance, the 2010 Stuxnet virus infected Iranian centrifuge controls through a flash drive loaded onto a single laptop within the air-gapped network used to manage the system. That work took relationship building, logistical smarts, and imaginative strategy, in addition to the sophisticated coding required. NICE has developed a Cybersecurity Workforce Framework that seeks to categorize the great variety of roles and functions that people in the field inhabit. Cutting across public, private, and academic sectors, the framework is meant to guide employers, educators, and workforce entrants in aligning their efforts with the overall needs of the field. Always a work in progress amid evolving needs and circumstances, the framework puts emphasis on competencies and skills. It is the default starting point for efforts to make cybersecurity visible and appealing to people who might consider it as a career option.
A 2018 Wall Street Journal headline captured the gist of these observations about working in cybersecurity: “Cybersecurity Requires ‘Insatiable’ Problem-Solving Skills; Technical Skills Can Be Taught.” The article recounted the proceedings of a “Cybersecurity Executive Forum” organized by the newspaper, in which field leaders identified their touchstones for cybersecurity career success. In sum, as one Chief Information Officer, noted, “Cognitive diversity is more important than anything for a cybersecurity person.”

Okay, fine. What does “cognitive diversity” really mean? Parsing the phrase through the filter of other comments and data points cited above, we might boil it down to two main elements: empathy, or the ability to inhabit other people’s views of the world; and imaginative, problem-solving skills.

Empathy is a starting point for any user-based design exercise. Understanding how someone else might use a tool, in different ways than are obvious to the designer,
always makes the tool better. A former Google engineer, Yonatan Zunger, put it this way:

“Since the whole purpose of the things we do is to fix problems in the outside world, problems involving people, that means that understanding people, and the ways they will interact with your system, is fundamental to every step of building a system.”

Problem-solving skills useful in cybersecurity build on empathy by combining a perspective of “other-ness” with the creative intelligence to improve or extend the efficacy of a security tool. Or, even better, break the tool. As “security guru” Bruce Schneier observes:

“Security requires a particular mindset. Security professionals – at least the good ones – see the world differently. They can’t walk into a store without noticing how they might shoplift. They can’t use a computer without wondering about the security vulnerabilities. They can’t vote without trying to figure out how to vote twice. They just can’t help it.”

The high stakes associated with cybersecurity systems make understanding how people might interact with them — with either constructive or nefarious intentions — all the more important. Achieving this understanding, then, requires blending the technical with the imaginative in ways that cybersecurity leaders find rare but crucial to their work.

To promote development of the technical skills cybersecurity professionals need, the National Security Agency has accredited just over 20 post-secondary schools as National Centers of Excellence in Cyber Operations. Many other schools leverage local industry connections and particular institutional strengths to offer cybersecurity education programs aligned with an understanding of industry needs. The University of Southern California has ties to Silicon Valley as well as the defense industry; Syracuse University offers concentrations in cybersecurity with finance applications; and Ohio State University links cybersecurity education to smart grids and mobile phone technology.
Chapter 5

FINDING KIDS WHO CAN AND WANT TO DO THE JOB

Connecting advanced cybersecurity-related technical training to the intangible, unconventional qualities of insight captured by the “security mindset” idea remains tricky, though. We would like to be able to identify students inclined towards a “security mindset” long before they reach higher education, at an age when their career interests and intellectual capabilities are still fluid and malleable. To grow the pool of potential cybersecurity professionals to a size that could meet the challenge of filling the 3 million-plus openings expected worldwide in coming years, we will need many more kids getting excited about the field than even all the 200,000 or so people who graduate every year with computer science and engineering degrees.

Getting kids aware of and excited about career opportunities in cybersecurity should therefore be an all-hands-on-deck effort. Computer science has rapidly gained a foothold in K-12 education, with dozens of states increasing their time and money commitments in recent years. This matters because the Computer Science Teachers Association includes cybersecurity in learning standards for computer science, and content embedded in standards gets tested. And content to be tested earns time in the school day, reaches large numbers of students, and becomes part of teachers’ knowledge base. Exciting, current work in
developing learning materials for formal education of this kind is starting to mature, as new ventures like TeachCyber are developing, in addition to programs of longer standing like Cyber.org and Hacker High School. In addition, the out-of-school environment is important, because it offers so much room for exploration and collaboration and hands-on experience in the field. Many organizations are stepping into this breach with afterschool-friendly resources, from bits’n’bytes to NOVA Labs to CyberPatriot, among many others.

The first step, though, can be the hardest to make: helping kids understand if they have an aptitude for cybersecurity work. How can we learn to identify — and help students self-identify as — budding cybersecurity whizzes? Of special importance is understanding that these special skills are not necessarily technical or computer-oriented. As Bruce Schneier observes, it has to do with seeing things differently, of imagining alternate uses — and misuses — of things more than it has to do with technical content or coding or networks and systems.

One approach to getting started with this work is to make it fun. Puzzles and brain teasers get everyone’s attention, and they can be great exercises for individual or group activities. Below is a selection of tricky but solvable brain teasers that draw on much the same kinds of aptitudes underlying Bruce Schneier’s “security mindset.” Students who can solve them – or even just enjoy them – might well be taking their first steps towards study and work in cybersecurity and innovations in information security that we could all benefit from.

Puzzles on the following pages are calibrated to elementary, middle, and high school levels, though all of them can pose enjoyable challenges at any age. They are inspired by, and in some cases, drawn from NCCAW activities meant to align with budding cybersecurity career aptitudes.
**ELEMENTARY SCHOOL**

1. What are the next two letters in the following series and why?

   W A T N T L I T F S __ __

   **Answer:** A and W – The whole string is made up of the first letters in each word of the question.

2. What letter is missing in the sequence?

   M, A, M, J, J, __, S, O

   **Answer:** A – Each is the first letter of a month of the year, starting with March, and A is for August.

3. What is the number missing from the last row?

   - 37, 10, 82
   - 29, 11, 47
   - 96, 15, 87
   - 42, __, 15

   **Answer:** 6 – In each case, the middle number is the sum of the digits of the two numbers on the ends. 4 + 2 and 1 + 5 both equal 6.
MIDDLE SCHOOL

1. What is the logic that connects these words in this order? (Hint: read them out loud.)

   gun, shoe, spree, door, hive, kicks, heaven, gate, line, den

   **Answer:** They all rhyme, in sequence, with the numbers 1 through 10.

2. What is the next number in this sequence?

   100  365  24  60  __

   **Answer:** 60 – These are units of time in descending order: 100 years in a century, 365 days in a year, 24 hours in a day, 60 minutes in an hour, and 60 seconds in a minute.

3. What is the next number in this sequence?

   77  49  36  18  __

   **Answer:** 8 – Each succeeding number is the product of the two digits in the number before it: 7 x 7 = 49; 4 x 9 +36; 3 x 6 = 18; 1 x 8 = 8
HIGH SCHOOL

1. Explain how 10 plus 4 equals 2.

**Answer:** When you’re looking at a clock, 10 o’clock plus 4 hours = 2 o’clock.

2. What is the next number in this sequence?

1, 11, 21, 1211, 111221, 312211, _ _ _ _ _ _ _ 

**Answer:** 13112221 – Each succeeding number describes the number coming before it, when you read them in order: 1 is one one, or 11; 11 is two ones, or 21; and so on.

3. Identify the next two numbers in the sequence below:

101, 112, 131, 415, 161, 718, _ _ _ _ _ _ _ 

**Answer:** 192 021 – Looking at the numbers as two-digit combinations, instead of three, will show them as 10, 11, 12, etc., up to 19, 20, and 21.

Solving tricky puzzles is obviously a long way from a technical cybersecurity credential. But the ability to see questions from a different angle, to find meanings in patterns that are obscure to others, does suggest the kind of supple, imaginative intelligence that equips cybersecurity professionals for success. A key for schools – and the cybersecurity workforce of the future to come out of them – is to embed learning along these lines within an educational pathway that can orient students towards opportunities in cybersecurity. The most obvious environment for such a learning pathway is within the STEM world, so let’s think about what a cybersecurity branch of the STEM tree might end up looking like.
Chapter 6

CYBER AND STEM ARE A GOOD FIT

Twenty or so years ago, when “STEM” started to take root in discussions about education and workforce policies and practices, computer science was nowhere in sight. It took more than 10 years for “CS” to become meaningfully associated with STEM. Cybersecurity, meanwhile, is scarcely a twinkle in the eye, included as noted in the form of a “subconcept” in computer science learning standards.

But the STEM story is a continuously evolving one. Thirty-three states committed over $40 million to K-12 computer science efforts in 2019 alone. Adding this “secret sauce” of technological innovation serves to reinforce and extend many of the reasons people put STEM forward as an answer to concerns about global competitiveness, workforce needs, and students’ learning and career prospects.

Cybersecurity education, it turns out, could well be a vehicle for reinforcing and extending reasons to include computer science within the STEM universe. Indeed, as a STEM discipline unto itself, cybersecurity education could reinforce arguments casting STEM education as a benefit to students and country alike. In the areas of career preparation, ethics, and multi-disciplinary learning, cybersecurity education can help engage students’ interests and ground their learning in a relevant context that is both intellectually rich and practically useful.

When people talk about plentiful STEM jobs, they are really talking about jobs in just a subset of STEM fields. The 150,000-plus students who graduate with life science degrees
every year vastly outnumber the not-quite 30,000 jobs projected to be open every year in the field. Likewise, the 167,000 or so social science graduates might need to sharpen their elbows to claim one of the 15,000 “social science” jobs available. On the other hand, the 72,000 computer science degree-holders will likely find a wealth of choices available to them among the over-400,000 computer occupations needing to be filled every year. Engineering degrees, too, match up well with job openings, though some fields more so than others.

So, in these lights, a STEM degree provides a far-from-certain pathway into a job that draws directly on the substance of a student’s major. As vocational training, we would have to say STEM education gets a middling grade.

We undersell STEM education, though, by pitching it as just vocational training. After all, a degree in a field does not necessarily signal an intention or desire to work in that field. Students often follow their nose one way in school and quite a different way after graduation.

Census Bureau data illustrate this point in vivid terms. A large-scale study comparing college graduates’ major field of study with their eventual occupations shows much less correlation between STEM studies and STEM careers than we might imagine. In no STEM field is the correlation between degree and job noticeably more than half, engineering and computer science included. A degree in physical science, for example, is about as likely to lead to work as a physical scientist as it is to work as a health care, management, or education professional.

STEM degrees, it would seem clear, can serve to launch students into a variety of careers far beyond the range of jobs implied by a particular major field of study. Especially in the less technical fields – i.e., non-computer and non-engineering – the career outcomes of STEM majors look much like those of non-STEM majors: people working in all sorts of fields doing all sorts of things. STEM education, writ large, seems to function well as broad-based preparation for career success in a wide variety of fields. The data visualization representing this study offers rewarding, abundant insights into this phenomenon.
WIDENING THE LENS

For those computer science and engineering degrees that do lead more often into related fields of work, though, something like the opposite issue arises: the education is too narrow. While imparting advanced technical expertise, education in these areas is seen as devoid of context. Students do not learn to consider the social dimensions or ethical implications of the high-tech products and services they launch into the marketplace.

Mitchell Baker, Chair and Co-Founder of Mozilla, laments the result of study in these fields that “produce[s] an environment where tech platforms and products [are] developed in isolation from the broader effects on society.” And indeed, dystopian applications of technologies are easy to find, coming in all kinds of flavors and scales:

- Facial recognition software has been repeatedly shown to have trouble identifying non-white, non-Western faces.

- Artificial intelligence tools are used to assess risk factors associated with defendants in court and make bail, sentencing, and parole decisions about them. These
algorithms are not governed by regulation or available for defense lawyers to inspect, effectively outsourcing legal judgments to private software developers with no necessary standing or qualifications within the legal system as a whole.

■ And, Facebook. Facebook. And Facebook.

A boomlet in “ethics in computer science” programs, in fact, seems to be taking shape in response to problems like these. Baker, for example, is leading a charge among philanthropic organizations and academics to identify and encourage approaches to integrating ethics into computer science programs. The Responsible Computer Science Challenge is delivering $3.5 million to undergraduate computer science educators working on this effort.

This argument puts something like John Dewey’s idea of “plasticity” at the center of a vision for STEM education: “The inclination to learn from life itself and to make the conditions of life such that all will learn in the process of living is the finest product of schooling.” Such learning how to learn, if you will, is a clear antecedent of the “21st-century skills” that people advocate in the interests of students, employers, and the country as a whole.

The mismatch between STEM degrees and jobs, the unexamined ethical dimensions of engineering and technology work, and “learning to learn” are all issues directly relevant to cybersecurity education. As it happens, a vision for cybersecurity education can stand on a foundation that encompasses all three of these dimensions:

■ Jobs: As we have observed, 3.5 million job openings are expected to be available in the field within the next couple of years. Accessible through certification, two-year, and four-year programs, these jobs cut across a spectrum of very-to-somewhat technical. Moreover, they do not include the 3-plus million jobs related to cybersecurity work that are currently in existence.
Ethics: With an explicit focus on understanding, preventing, responding to, and recovering from cyber attacks, cybersecurity jobs are designed to keep individuals and organizations safer online. The field, it could be said, operates with an inherent sense of ethical purpose, and professionals in the field make decisions and take actions with this purpose always in mind.

“Plasticity”: Because online threats are constantly evolving in response to preventive measures and new technologies, the imperative to learn from experience and circumstance is urgent in cybersecurity work. Leaders in the field tout critical thinking skills, curiosity, and inventive thinking as vital attributes for success in the field. Technical skills, meanwhile, can be taught.

Cybersecurity education, in its fullest implementation, would cut across multiple, varied disciplines. Business, law, and math are obvious points of contact for cybersecurity learning programs, but the opportunities for crossing subject matter boundaries go further. John McCumber’s argument about the virtue of broad-based education can serve as a bearing point towards which cybersecurity education leaders might direct their programs. Such a widened approach, we have tried to argue, would not only serve employers’ and society’s broader needs but also serve to enhance the appeal and accessibility of cybersecurity for exactly the larger, more diverse audience of students we need to reach.
Chapter 8

HOW WE WOULD LIKE TO HELP

We developed our Cyber Career Awareness Program, or CyberCAP, to provide advocates and practitioners of cybersecurity education with a starting point for showcasing the field to middle- and high-school students as a possible career pathway. It consists of a career guide, student workbook, and teacher’s guide designed to support educators even with no background in the field.

The Cybersecurity Career Guide features current news items and trends in the field, in-depth explorations of what professionals in the field actually do, and extensive coverage of opportunities in post-secondary education and workplaces. The workbook ranges from individual online safety principles and practices to exercises in reasoning, ethics, and role-playing to individualized career assessment and planning activities. And the teacher’s guide includes learning objectives and supplemental content, time estimates and discussion questions for planning lessons, and substantive guidance for getting the most out of the program.

The program emphasizes concepts and principles over technical content. It is designed to engage and appeal to students of all backgrounds and interests. We believe it reflects the incredible variety of opportunities and rewards that cybersecurity work can offer. And it can serve as an opening statement to student audiences that require new and different presentations of the field to make them look twice, or even once, at what it has to offer. If you’re interested in learning more or seeing a sample of the program, please be in touch. You can find us at start-engineering.com.