## Turning a national problem into student opportunities

Introducing PLTW's new Cybersecurity course

National issues involving cybersecurity are in the news and on the rise – from the Equifax data breach that compromised the personal security of almost half the country, to mega breaches involving retail giants Target and Home Depot. Globally, the annual cost of such data breaches is expected to increase to $6 trillion by 2021, leaving businesses across all sectors grappling with how to protect their customers and employees.

A global cybersecurity workforce shortage is adding to the challenges businesses face as they seek to protect themselves against cybersecurity threats. The 2017 Global Information Security Workforce Study, released in June 2017, shows that the cybersecurity workforce gap is on pace to hit 1.8 million by 2022 – a 20 percent increase since 2015. Two-thirds of the study's participants indicated that there are not enough cybersecurity workers in their organizations to meet the challenges they currently face.

As a result, cybersecurity professionals are in high demand. The Bureau of Labor Statistics has projected that computer and mathematical occupations will grow at a much faster rate than other occupations between 2016-2026, but industry demand is quickly outpacing the supply of workers who have the necessary skills and expertise.

Project Lead The Way (PLTW) is committed to providing an inspiring and inclusive K-12 computer science experience that empowers students, preparing them with the in-demand knowledge and transportable skills they need to thrive in a rapidly evolving world.

### Cybersecurity – Unique Benefits of PLTW's New Course

- **Sparks Interest and Fosters In-Demand Skills**

  *Whether seeking a career in the growing field of cybersecurity or learning to defend their own personal data or a company's data, students in Cybersecurity establish an ethical code of conduct while learning to defend data in today's complex cyberworld.*

  The course is designed to expose high school students to the ever-growing and far-reaching field of cybersecurity by providing students with inspiring and relevant learning experiences, during which they train and solve real-world problems as cybersecurity experts do.

  The course provides students with a broad exposure to the many aspects of digital and information security, while encouraging socially responsible choices and ethical behavior. It inspires algorithmic and computational thinking, especially "outside-the-box" thinking. Students explore the many educational and career paths available to cybersecurity experts, as well as other careers that comprise the field of information security.

- **Introduces Relevant Cybersecurity Skills in an Engaging, Secure, and Responsible Way**

  - *Network Security Lab*
    In the classroom, students will explore operating systems and networks in isolation from any school or district network. Through the course's Network Security Lab, students and teachers will have access to a completely isolated, secure, and legal environment for exploration and learning to gain hands-on cybersecurity skills. As students interact with their teams in this simulated environment, they will discover how the skills they're learning can help them solve real-world problems like cybersecurity experts do, while experiencing the relevancy of these skills.

  - *Well-Known Exploits*
    All of the vulnerabilities that students will learn are well-known and well-defined exploits – a term used to define a software tool that takes advantage of a flaw in a computer system. These are easily identified and denied by today's basic anti-virus software, meaning that schools or district networks will not be at risk. Information Technology departments will be given a "whitelist" of sites that students will need to access from within the virtual system.

  - *Ethical Approach*
    An ethical approach to cybersecurity concepts is a key priority for the Cybersecurity student experience. Students will learn that ethical and responsible practices of cybersecurity are highly valued in society and by future employers. At the same time, they will learn that unethical and reckless hacking may get them banned for life not only in a cybersecurity career, but in other, unrelated careers as well. One of the first activities students will complete as part of this course is a class Code of Conduct based on industry- and PLTW-recommended best practices for cybersecurity.

- **Connected to Industry and Aligned to Standards**

  PLTW courses are designed to empower students to thrive in an evolving world. As part of this process, we take industry connection and standards alignment into account when developing our curriculum.

  The development of Cybersecurity was informed heavily by the National Cybersecurity Workforce Framework (also known as the NICE Framework or NCWF). Created by the National Institute of Standards and Technology (NIST), this framework identifies standards that have been developed by numerous academic, industry, and government organizations. The framework objectives address topics that span K-12 education and guide learning progressions.

  The NICE Framework defines Knowledge, Skills, and Abilities (KSAs) that are required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training. Cybersecurity aligns to Abilities that are relevant to high school students' education.

  The Cybersecurity course content also aligns to CSTA K-12 standards, K-12 CS Frameworks and Common Core State Standards for Mathematics and English Language Arts.

- **Ensures Access to the Most In-Demand and Relevant Experiences**

  In order to empower students with the skills they need to thrive in college and career, PLTW works closely with educators and industry to develop and validate its programs, ensuring that PLTW programs are the standard in career learning. As part of this process, PLTW evaluates and verifies which in-demand, transportable skills leading companies need in their workforce and integrates these competencies and skills – such as problem solving, critical and creative thinking, communication, and collaboration – into the classroom experience.

  The Cybersecurity course's advisory board, which includes national experts from industry and education, as well as leaders from government and research institutions, has been critically important in curriculum development to ensure students have access to the most in-demand and relevant experiences in a field that is rapidly evolving every day.

- **Provides More Opportunities for Students to Engage in Computer Science**

  Cybersecurity is a full-year course recommended for students in grades 10-12. Cybersecurity offers high school students the opportunity to experience the many aspects of digital and information security that are critical to encouraging academic study and career awareness. Offering this opportunity at an earlier age is especially important for young women, as research shows they are deciding against careers in cybersecurity before age 16. Another important aspect to consider is the students' ability to act responsibly in their decision-making and understand the short- and long-term implications of their actions. Therefore, we recommend implementing Cybersecurity as early as 10th grade to provide timely access to students and increase their motivation and career consideration in an ethical and responsible way.

  The Cybersecurity course is part of PLTW's full and comprehensive 9-12 solution for computer science. In addition to Cybersecurity, PLTW offers three other courses within the PLTW Computer Science program: Computer Science Essentials, Computer Science Principles, and Computer Science A. With PLTW Computer Science, you can choose to start with a single course, implement all four courses, or anything between.

  If your school is considering sequenced implementation, there are different approaches to consider:

  - You could start by offering Computer Science Essentials, followed by Cybersecurity, Computer Science Principles, and Computer Science A. This option provides students with a strong computer science foundation before they start taking more advanced programing courses.

  - Another option is to offer Computer Science Essentials, followed by Computer Science Principles, Cybersecurity, and Computer Science A. This option allows students to build on fundamental concepts, broaden their scope by diving into a specific field, then progress to a more advanced programing course.