Broadening and Diversifying the Reach of Cybersecurity Education

Abhilasha Bhargav-Spantzel, Principal Engineer, Intel Corporation
David Bills, Director of Academic Programs, Intel Corporation

Cybersecurity education is of prime importance in today's world. Increasing threats from attackers are motivated by financial and other gains, and these bad actors have access to advanced tools, resources and services from the hacker community.

This growing problem is evident in numerous news reports on the impact of cyber-attacks on individuals and organizations across the globe, and it will only get trickier as more digital devices and services become available in the future. These challenges, coupled with the shrinking talent base of solutions expertise, highlight the importance of broader cybersecurity education.

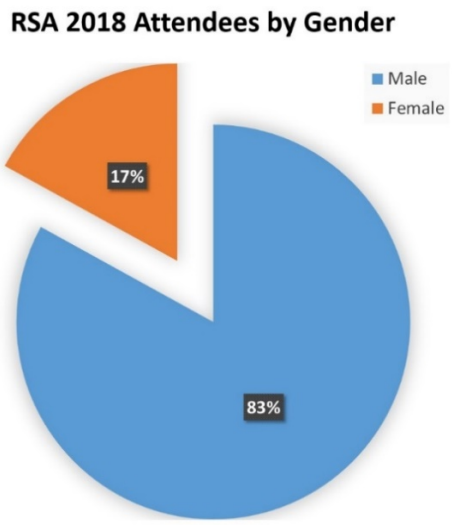
We need a comprehensive and granular approach. While no single individual is an expert in all cybersecurity areas, **foundational elements** can help provide the needed professional skills. This foundation should foster deep knowledge of the history and origins of cybersecurity challenges and solutions, as well as a good **understanding of their diverse range and interdisciplinary relevance**.

For decades, we've seen **significant research and security assurance initiatives**—from the U.S. Department of Defense Orange Book in the 1980's to the European Union's General Data Protection Regulation (GDPR) today. These efforts point to the network security protocols, system security design principles, privacy enhancing technologies, threat modeling, and other foundational elements for cybersecurity education. These must be coupled with an understanding of **today's compute platform**, not only **PCs** and **cloud** servers, but also internet of things (**IoT**) devices, connected **cars**, and the **ever-evolving world of digital services**.

This broader education effort must be grounded in how cybersecurity impacts us in both the **cyber and physical world**. The corresponding importance of **safety, privacy** and the **long-term consequences** to individuals and to society must also be considered.

To develop such a comprehensive approach, we need to nurture a diverse group of individuals—both teachers and students—to motivate and strengthen the defenses that become part of the design in every engineer's respective field. There is **no one-size-fits-all to attract the diverse set of individuals,** so one must **employ targeted tactics to attract** specific groups of **individuals.**

The lack of diversity evident at RSA-2018, where women comprised only 17 percent of attendees, points to a problem that needs to be tackled**. "Failure of imagination**" has been cited as the reason we were caught off-guard by the Russian interference with the 2016 U.S. presidential election, and the same was said about Sept. 11, 2001. By bringing more types of



people with a more diverse range of experiences and backgrounds into protecting our security, we can broaden the imagination brought to bear on future threats, especially in the cybersecurity domain.

We as society have yet to understand the full impact and cost of decisions made yesterday, today regarding **privacy**. We must think this through completely and how it will **impact our future** and the future of generations to come. If we are not careful, we will see our **technologies weaponized** which makes nuclear warfare obsolete. A scary proposition!

Finally we need to **future proof** our education system. The **education system** has never moved at the **speed of technology** and business and this must change. Education must have **a sense of urgency** and move at a faster pace. As part of growth mindset – we need to get out of the old mentality of how school is run. One way is to **partner with industry** to understand the pain points and quickly **develop the curriculum to bridge the gap**. **Education meets real-world experience and moves at the speed of business**. This has to be tackled carefully to **avoid "shiny object syndrome"** and ensure the due diligence is done to tackle the underlying problem. The education goes both ways, similar to many feedback loops in carefully designed security and risk management systems to allow continuous education opportunities for all.

It is great to see strong cybersecurity education efforts by notable leaders academia, government and industry. For example, Intel is leading initiatives with the academic community to bring diversity to high-tech in general and cybersecurity in particular. We focus on **outreach programs** to universities and students of **all genders, backgrounds, interests** and various majors to talk about the comprehensive cyber security considerations.

Training cybersecurity professionals is now more critical than ever. A recent government and industry Task Force is predicting that 1.8 million cybersecurity-related positions worldwide will go unfilled by the year 2022. Building collaborative programs and ensuring diversity of representation in these programs would be critical in **addressing this shortfall** in needed professionals to tackle the challenges and **win on our path ahead.**

Abhilasha Bhargav-Spantzel is an Intel Principal Engineer focused on identity, security and privacy. She has numerous patents and broad experience in identity management, cryptography, biometrics, hardware devices and system security. She leads multiple diversity and inclusion efforts at Intel, and actively drives development of women in engineering and cyber security. Find her on LinkedIn.

David Bills is the Director of Academic Programs for the Platform Security Division where he collaborates with academia to drive security research, education, and talent acquisition. For the past 2 years, he has served on Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) board. David built Intel's scale ISV software enabling ecosystem from prior to his academic work. LinkedIn