

BRIDGING THE TALENT GAP

HOW THE PHILIPPINES
IS COPING WITH THE
OVERWHELMING
DEMAND FOR CYBER
SECURITY PROFESSIONALS

By **Genalyn B. Macalinao**, information technology officer, Philippine Department of Information and Communications Technology

Lockdowns around the world have placed economies at a standstill, slowing the virus's spread but causing a heavy economic toll. In the Philippines, an overwhelming majority of companies are encouraging or requiring their employees to work from home because of COVID-19, so it's no surprise that cyber security and data privacy issues have started to surface.

Never before has the country's lack of cyber security professionals been more glaring. While the issue has been brought up several times by cyber security stakeholders, it is in this national emergency that everyone in the country felt the dire need for a strong cyber security infrastructure and a workforce capable of ensuring continued operations of the government and other critical infrastructure.

Workers across the information technology (IT) sector are needed more than ever to enable governments and critical infrastructure, help businesses stay online and keep citizens connected. Cyber security professionals are critical to supporting health care providers, manufacturing technology

products and components, securing and servicing critical data centers, delivering food and essential needs to communities, keeping out-of-school students engaged, and enabling governments to respond to this global health crisis.

At a time when their skills are essential, there's a major gap between the number of qualified cyber security workers and what is needed. Even before the onset of the pandemic, Cybersecurity Ventures projected that the shortage would spark an industry crisis with a staggering 3.5 million unfilled positions by 2021. In 2016, the Philippines trailed its peers in the Association of Southeast Asian Nations with only 84 Certified Information Security Systems Professionals (CISSP), according to (ISC)². Indonesia had 107, Thailand had 189, Malaysia had 275, and Singapore had 1,000. On top of this, half of the 84 Filipino CISSPs were reported to be working overseas. A study conducted by IBM and the Ponemon Institute in 2018 showed the cyber security talent deficit carries immense risks as the number of sophisticated data breaches increases without competent professionals to

detect and prevent attacks. Testament to that are a number of high-profile cyber security incidents and data breaches that have plagued the Philippines one after another.

A prime example is the data breach of the Commission on Elections. On March 27, 2016, hackers under the banner “Anonymous Philippines” hacked into the website of the Philippine Commission on Elections and defaced it. The hackers left a message calling for tighter security measures on the vote-counting machines to be used during the May 9, 2016, Philippine general election. Without a cyber security plan in place, the country was left at the mercy of cyber criminals.

A month after the elections, the law creating the Department of Information and Communications Technology (DICT), Republic Act No. 10844, was signed.

- The protection for supply chains through a national common criteria evaluation and certification program.
- The protection of individuals through the acceleration of learning skills and development, a cyber security outreach project, a national cyber security awareness month, and equipping the government and the program for local and international cooperation.

The Cybersecurity Bureau of the DICT conducts roundtables with the 12 CII sectors (government, information communications, energy, aviation, maritime, land transport, health care, banking and finance, water, security and emergency, media, and business process outsourcing), inviting the academe for awareness on industry needs. It is this endeavor



To further engage Philippine youth in cyber resiliency initiatives, the Department of Information and Communications Technology coordinates with the Department of Education to integrate cyber security curriculum in senior high schools.

Eliseo Rio Jr., left, then acting secretary of the Department of Information and Communications Technology, and Felizardo Colambo, president of AMA Computer University Inc., sign an agreement in 2019 meant to increase the number of cyber security professionals.

PHILIPPINE DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

The DICT is a government agency tasked to develop policies and plans for information and communications technology (ICT) development in the country. It exercises broad powers over telecommunications and broadcasting, cyber security, data privacy, consumer protection, and the promotion of trade and investment in ICT and ICT-enabled services. The department was barely a year old when it launched and published the National Cybersecurity Plan (NCSP) 2022, a five-year plan that serves as the country’s road map to its vision of a cyber-resilient Philippines.

The NCSP provides the foundation for cyber security policy-making, covering the implementation plan. Key strategic initiatives were laid out, featuring a holistic and multilayered response system to better protect critical infrastructure against cyber threats. A key imperative of the National Cybersecurity Plan is to support the development of cyber security professionals.

The NCSP 2022 sets out the following key program areas to address the need for increased awareness and capacity building for the public and private sectors:

- The protection of critical information infrastructure (CII) through cyber security assessment and compliance, national cyber drills and exercises, and a national database for monitoring and reporting.
- The protection of government networks through a national computer emergency response program, a capacity building and capability development program, a pool of information security and cyber security experts, the Threat Intelligence and Analysis Operations Center, protection of electronic government transactions, and the update of licensed software.

that paved the way for partnerships with the academe in the development of cyber security curricula.

The bureau also sits on the technical panel of the Commission on Higher Education (CHED) for the development of policies, standards and guidelines (PSG) for the bachelor’s program in cyber security. The PSG is now in its second draft and is currently in the consultation phase.

While waiting for the release of CHED’s PSG for the Bachelor of Science in cyber security, the DICT is continuously appealing to schools to integrate cyber security into their curricula.

Some institutions now offer new cyber security courses. This is part of the Philippines’ efforts to strengthen students’ skills in science, technology, engineering and mathematics (STEM). As the first IT school in the Philippines, it is no surprise that AMA University is the first school in the country to offer a bachelor’s degree in cyber security. This was realized through a partnership with the DICT Cybersecurity Bureau and inspired by the cyber security curriculum developed by the George C. Marshall European Center for Security Studies. In response to the need for formally educated cyber security professionals, AMA University is now accepting enrollees at its main campus in Quezon City, Philippines. An initiative from the private sector is the partnership between the security firm Palo Alto Networks and Asia Pacific College to launch the first cyber security academy in the Philippines.

While some schools in the Philippines have integrated cyber security into their curriculum, much still must be done to bridge the huge gap between industry needs and a cyber security workforce with the right skills. □