- Computer crimes

Cyber security

Manila Bulletin · 4 May 2018 · B3

Undoubtedly, cyber security is becoming a priority concern across all industry in this digital age. The hackers are becoming more sophisticated. IT expert Winnie Chan tells me anybody and anything that has an IP address can be remotely hacked. Anybody who has an address can be broken into.

I know it's the first Friday of the month and as I was raised as a Roman Catholic, I distinctly remember my grandmother telling me to go to church, including confession. Having said this, allow me to make two confessions: First, I've been a victim. Not once but thrice, my email add was hacked with attackers asking my friends and those in my contact list for monetary help because I lost everything and as a result I was marooned in a foreign country. Second, I am no tech-savvy. I may have topofthe-line gadgets but whenever I get hold of new ones, I would seek the assistance of Pangga, my 15-year-old grand daughter, or Jackie and, Eloisa to guide me through its menu.

Victimized and following the introduction of financial technology (fintech) in the corporate world and the attendant need to fortify cyber security due to the increasing incidents of cyber crimes/fraud, these, two topics sparked my interest. As per the advice of Mr. Chan, it "starts with awareness." Though I am still under the weather, I attended the half-day forum sponsored by MayBank Philippines on "Managing Cyber Security in the Age of Digital Transformation" with Bangko Sentral ng Pilipinas (BSP) Deputy Governor for bank supervision and examination Chuchi Fonacier giving the keynote address. The forum was educational and an eye-opener for non-tech savvy individuals like me.

Ms. Fonacier aptly described the state we are all in right now as a "cross roads." Technology presents a "double edged sword with beneficial advantages on one side, and cyber threats and risks on the other." Considering the "high-profile cases of cyber attacks continually dominating the news," and in "an increasingly complex and sophisticated fashion," one of which hit the Philippine financial shores, the BSP official said she believed "a holistic government approach to cyber security involving various national, local as well as other government agencies must be carried out to broaden its scope and effectiveness."

Listening to the other speakers, Department of Information and Communications Technology Assistant Secretary Allan Cabanlong and Singapore-based certified information security manager and director of Asia Financial Series Sharing and Analysis Center Robert Poh, there's another emerging dimension, concern to cyber risks- Artificial Intelligence (AI). Cyber security is absolutely critical to the whole digital world, including AI. Specifically, Mr. Cabanlong says AI is meant to make our "work easier" but never to "replace humans."

AI has three main parts – data, algorithm, and predictive judgment. If any of the two parts get altered then the third part gets damaging, especially in a healthcare setting when an AI tries to interpret an x-ray result. I learned that most of the cyber attackers are using AI to hide behind the cloak of their surreptious activities.

I left the forum more learned on cyber security, which has become an important component of any business now more than ever. As an antidote to all these hackings and the need for more protection in the digital space, Vic Yap, a friend who is IT savvy says the current trend right now is to engage a chief information security officer.

Indeed, as in any other undertaking, there is no room for complacency.

Talk back to me at sionil731@ gmail.com