Dr. Fu-Long Tsai: Applications of AI in Financial Industry

Organizer: Department of Computer Science and Information Engineering

Time: December 16, 2022

Venue: G315, Main Engineering Building

Speaker: Dr. Fu-Long Tsai, Secretary General of Financial Supervisory Commission

Subject: Theory and Practice of Financial Technology - Application in Industry and Trend

Because of the high utilization of information technology in the financial industry, coupled with the prevalence of remote work, people's demand for using the internet is increasing day by day. There is always a risk of internal network systems being accessed or even further attacked, causing a large number of hackers to emerge from all sides. In addition, financial institutions also need to be subject to strict management on the business level when it comes to investment operations. In order to avoid unauthorized downloading or access, for example while working remotely from home, certain tasks related to customers' personal information cannot be processed, leading to delays in some work progress.

Although there are no absolute security measures for finance-related cybersecurity issues, it is possible to strengthen security measures through more resilient means. Some may not understand the usage of "resilience" in this context. It is one of the popular terms this year, and "cybersecurity resilience measures" refers to measures that prevent hackers from easily invading and stealing accessed data, and can effectively prevent future risks.

At the same time, he also summarized the following resilience measures: data backup, regular information security drills and awareness-raising, outsourcing management, IoT management, identity authentication, VPN remote office management, overall architecture of financial DDoS and CDN, and enhancing the defense capabilities of small organizations. Among them, the simplest and most common measure is to access backup data offline, in a third location, or on cloud storage, to prevent important data from being lost. Adopting a zero-trust network, which follows the principle of "never trust, always verify", and implementing network segmentation and rigorous access controls, is also a good measure. As for the establishment of a virtual monitoring emergency command center responsible for 24/7 information security monitoring, I believe this is the most practical and effective method.

Taiwan's financial cybersecurity action plan is being promoted in 5 directions: public-private collaboration, differentiated management, resource sharing, incentive measures, and international cooperation. The government can work together with various industry associations to cooperate and divide the work according to different types of cyber security needs, and also collaborate with other countries' cybersecurity organizations to establish mutual intelligence sharing and better grasp the international cybersecurity situation and context. Our government actively promotes an organizational culture that values cybersecurity, and continuously encourages the establishment of cybersecurity units or personnel and the appointment of directors or advisors with cybersecurity backgrounds. The legislation was amended in September 2021, and currently, 39 domestic banks, 8 insurance companies, and 13 securities firms have established chief information security officers (CISOs); 41 insurance companies, 39 banks, and 3 securities firms have set up dedicated cybersecurity units; and 48 financial institutions have appointed cybersecurity consulting teams to actively implement and promote measures to achieve the effectiveness of cybersecurity protection.

Finally, I believe that systematic cultivation of financial cybersecurity professionals to enhance public awareness of cybersecurity is an essential aspect of life. For example, cultivating interdisciplinary talent,

increasing the number of cybersecurity teachers in relevant fields in schools, and encouraging cybersecurity personnel to obtain relevant certifications to enhance their professional abilities, are all important steps. I hope to strengthen the assessment and management of risk in the financial supply chain system and urge people consider any potential cybersecurity risks when promoting emerging technology businesses. This includes revising cybersecurity self-regulatory standards, strengthening cybersecurity protection for emerging technologies, and balancing service innovation and security. Don’t get caught up in unnecessary cybersecurity risk wars due to momentary negligence or a desire for urgent innovation. Dealing with these issues will require extra effort and time. I would like to thank the students for their attention, and I hope that this speech can provide you with practical help in the future!

2023/03/16