Woodpecker Technology 產品總監 張智凱博士：Cybersecurity Market Survey: Products, Services, and an Emerging Trend

文／翁健棋

隨著網路科技的蓬勃發展，人們對於網際網路的依賴程度越來越高。然而，網路的普及也同時帶來了新的風險和挑戰，近年來頗受社會大眾關注的「網路安全問題」便是其中一例。據統計，全球網路使用者已經超過 40 億人，而每年因網路攻擊所造成的經濟損失高達數十甚至數百億元。不僅如此，網路攻擊手段也越來越多樣化，從惡意程式、網路釣魚到身份盜用等，都對個人和企業的資訊安全構成了威脅，網路安全意識和各項措施的補強可謂刻不容緩。

有鑒於此趨勢，本院資訊科學與工程研究所於去年底舉辦一場以「Cybersecurity Market Survey: Products, Services, and an Emerging Trend」為主題的論文研討會，由於本校取得博士學位，現任職於 Woodpecker Technology 公司，擔任產品總監的張智凱學長擔任主講人。張智凱學長曾任富士康的網路安全解決方案團隊負責人，並於 2015 年至 2016 年期間擔任 IEEE Reliability Magazine 的助理編輯。不單如此，張智凱學長還曾擔任本校亥客書院、HITCON Community 2018 和其他相關培訓計劃的網路安全講師，是極具資格與歷練經驗的合適主講人選。

本次研討會主要希望能協助聽講者了解資安市場及其相關產品、服務和趨勢，以期對未來的學習和研究有啟發作用。於研討會開頭，張智凱學長列舉數項網路安全市場中的防禦產品，點出企業對於「免受網路攻擊之防禦系統」的需求和重要性，藉此帶出開放網路軟體安全計畫 OWASP （Open Web Application Security Project）所推崇的 Cyber Defense Matrix（CDM）框架。該矩陣架構列出了幾個關鍵區域，如預防、偵測、反應和恢復，並將每個區域細分為不同的部分，幫助企業更好地了解所需的安全產品和服務，並制定適當的保護措施，避免遭受惡意網路攻擊。

緊接著，張智凱學長談到資安可視性（cyber security visibility）的概念，引用孫子兵法名句：「知己知彼，百戰不殆。」闡釋除了對外部威脅的監控與預防，清楚了解自身的各項資產並洞悉相關風險和漏洞亦十分重要。舉例來說，從產品的硬體資訊到程式運作情形、用戶帳號使用狀態、網路流量，皆是建構資安可視性的重要資料。然而，根據 Forrester 組織的市調研究，現今只有約 17% 的組織落實資安可視性的部署，其原因便在於資安學術圈領先資安應用圈很長一段距離，導致很多新技術在產品化時會有一道較難跨越的檻，無法將最新的技術妥善運用，達到資安防護效果。

於研討會末段，張智凱學長談及由 AI 驅動的安全可視性技術之優缺點。對於企業和組織來說，使用人工智慧來監控、分析數據，可以大幅降低對人力資源的依賴，從而節省時間和人力成本。不僅如此，還可以透過對大量數據進行分析和比較，快速識別不正常的行為或模式，提前預警潛在的安全威脅，從而避免因攻擊帶來的損失和損害。然而，此技術也存在一些缺點和挑戰，包括其需大量的數據來支撐和培訓模型，以及 AI 模型和算法可能存在偏差，導致分析和預測結果出現誤判等，皆是尚待優化、解決的問題。

總的來說，AI 驅動的安全可視性之相關技術深具發展潛力，可以幫助企業和組織更好地保護數據安全，使其能及時發現和處理潛在的安全威脅。然而，相關部門在實施前仍需仔細權衡其利弊，同時採取必要的安全措施來確保數據的安全性和可靠性，方能落實「知己知彼」策略，實踐網路安全防護！

Dr. Chih-Kai Chang's speech on Cybersecurity Market Survey: Products, Services, and an Emerging Trend

As internet technology continues to thrive, people's reliance on the internet is increasing. However, the popularity of the internet also brings new risks and challenges, and "cybersecurity issues" have become a topic of concern for society in recent years. According to statistics, there are now over four billion internet users worldwide, and the economic losses caused by cyber attacks reach tens or even hundreds of billions of dollars each year. Not only that, cyber attack methods are also becoming more diverse, from malicious software, phishing, to identity theft, all of which pose a threat to individuals and companies' cybersecurity. Therefore, strengthening cybersecurity awareness and measures is urgently needed.

In light of this trend, the Institute of Computer Science and Engineering at NYCU held a seminar last year on "Cybersecurity Market Survey: Products, Services, and an Emerging Trend." The keynote speaker Dr. Chih-Kai Chang is an experienced speaker to talk about this topic. He obtained his doctoral degree at NYCU and currently serves as the product director at Woodpecker Technology. Dr. Chang previously served as the head of a cybersecurity solution team at Foxconn and was an assistant editor of IEEE Reliability Magazine from 2015 to 2016. Moreover, he has also served as a cybersecurity lecturer at College of Hacker, HITCON Community in 2018, and other related training programs.

The purpose of this seminar was to inspire future learning and research in the field of cybersecurity through guiding the audience in learning about the cybersecurity market and its related products, services, and trends, with the hope of inspiring future researchers in this field. At the beginning of the seminar, Dr. Chang emphasized the importance and demand for defense systems against cyber attacks among companies. He listed several categories of product available in the cybersecurity market. Dr. Chang then introduced the Cyber Defense Matrix (CDM) framework promoted by the Open Web Application Security Project (OWASP). The CDM framework lists several key areas such as prevention, detection, response, and recovery. Each area is subdivided into different parts to help companies better understand the required security products and services. This framework can help companies formulate appropriate protective measures to avoid malicious cyber attacks.

Next, Dr. Chih-Kai Chang talked about the concept of cyber security visibility. He cited a famous quote from Sun Tzu's The Art of War: "know yourself and know the enemy, and you can fight a hundred battles with no danger of defeat." He then explained that in addition to monitoring and preventing external threats, it is also important to have a clear understanding of one's own assets and to be aware of related risks and vulnerabilities. For example, data such as hardware information, program operations, user account usage status, and network traffic are all important for building cyber security visibility. However, according to market research by Forrester, only about 17% of organizations currently have implemented cyber security visibility. One of the possible reasons is that cybersecurity in the academic field is still ahead of cybersecurity applications in reality. As a consequence, many new technologies face challenges in productization, making it difficult to utilize the latest technologies to achieve cybersecurity protection efficiency.

In the final stages of the seminar, Dr. Chih-Kai Chang discussed the advantages and disadvantages of AI-driven security visibility technology. For enterprises and organizations, using artificial intelligence to monitor and analyze data can greatly reduce dependence on human resources, thereby saving time and labor costs. Moreover, through analyzing and comparing large amounts of data, abnormal behaviors or patterns can be quickly identified, potential security threats can be detected in advance, and losses and damages caused by attacks can be avoided. However, this technology also has some shortcomings and challenges, including the need for a large amount of data to support and train models, as well as the possibility of bias in AI models and algorithms, which can lead to misjudgments in analysis and prediction results, and these issues need to be optimized and resolved.

Overall, the related technologies of AI-driven security visibility have great development potential and can help enterprises and organizations better protect data security. In addition, potential security threats can be dealt with and detected in a timely manner. However, each company or organization needs to carefully consider the pros and cons before implementation. Furthermore, it would be better to implement necessary security measures to ensure the security and reliability of data, as the strategy "know yourself, know your enemy" suggested by Dr. Chang for network security protection.