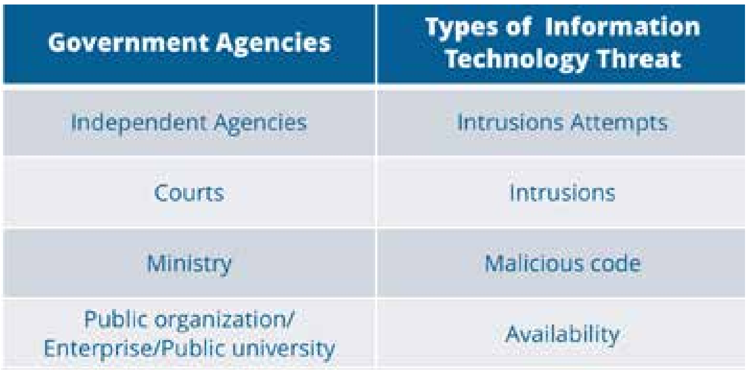
CYBERSECURITY THREATS IN THAILAND

By Yada Saraneeyatham

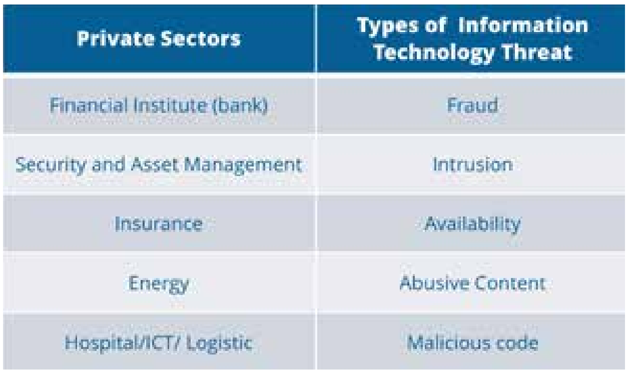
Cybersecurity threats in Thailand are intensifying and their current cybersecurity ranking, worryingly, is falling to new lows. All these infections and security breaches come as at a cost and the potential cost to Thailand alone close to $500 million from the direct and indirect cost of fraud and breaches. According to the 2020 Global Cybersecurity Index (GCI) by the International Telecom Union, Thailand ranked 44 out of 194 countries, where its reputation dropped further from ranking 35th in 2018. It is estimated that Thailand spent around $360 million on cybersecurity expenditure in 2021 with expected growth rate of 7.7%. Currently, Thailand cybersecurity spending consists of the expenditure on identity and access management, infrastructure protection, and network security.

In 2021, Thailand Computer Emergency Response Team (ThaiCERT) under Electronic Transaction Development Agency (ETDA) reported that there were total of 2,065 cyber threat incidents, where vulnerability accounted 32% and malicious code accounted 23% out of total incidents.

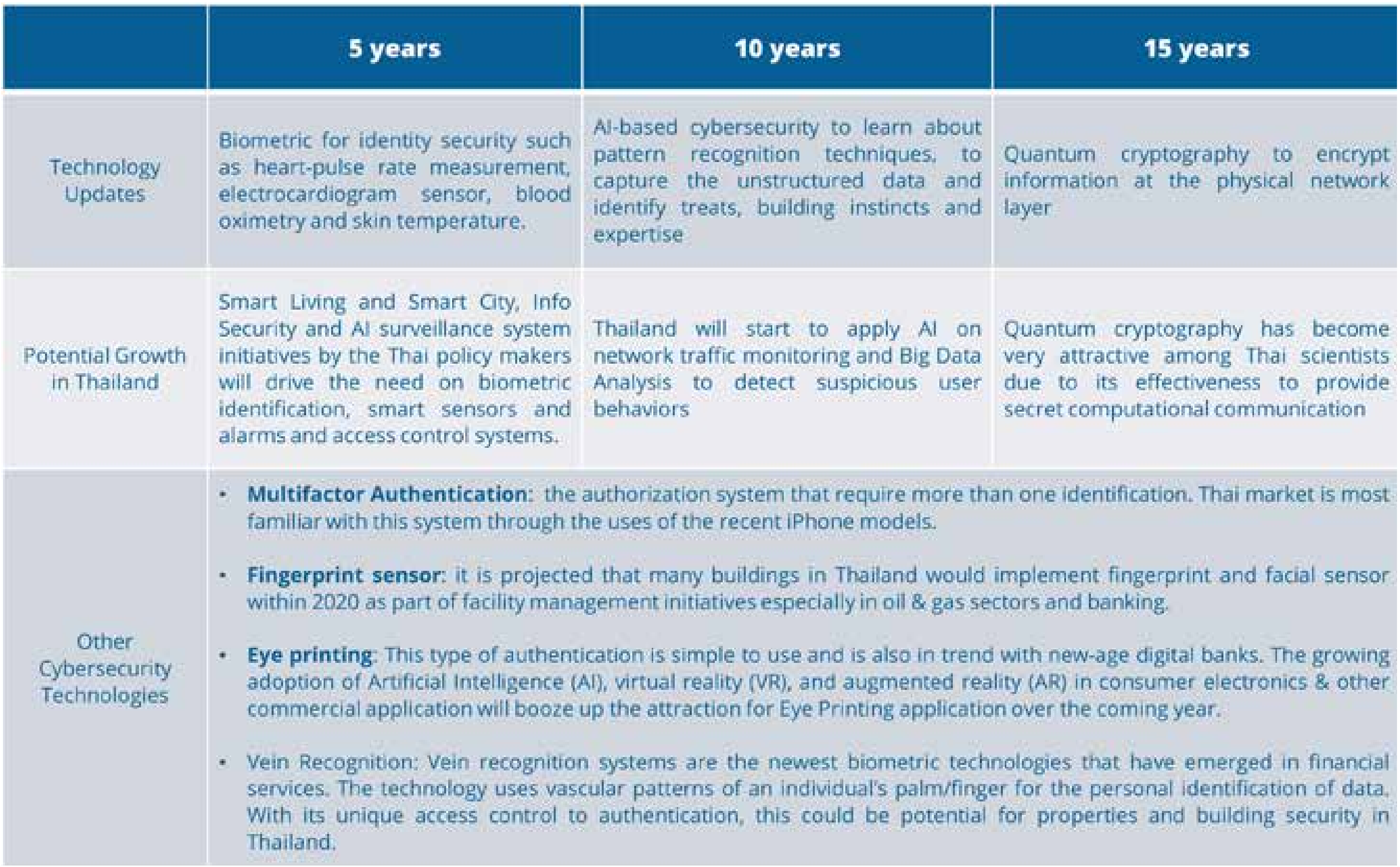
Government agencies are often targeted for massive data breaches such as personal identification card details and medical records from public hospitals. Meanwhile, corporate groups and businesses have always been the main targets of cybercrimes by money-motivated cyber criminals. This is especially the case during the pandemic where employees have been working remotely from home. Surprisingly, it is the large businesses themselves that are most at risk. The three most concerning cybercrime tactics targeting corporations include brand impersonation, data exfiltration, and data corruption. These have the highest impacts on businesses with the slowest



Government Agencies	Types of Information Technology Threat
Independent Agencies	Intrusions Attempts
Courts	Intrusions
Ministry	Malicious code
Public organization/ Enterprise/Public university	Availability



Private Sectors	Types of Information Technology Threat
Financial Institute (bank)	Fraud
Security and Asset Management	Intrusion
Insurance	Availability
Energy	Abusive Content
Hospital/ICT/ Logistic	Malicious code



	5 years	10 years	15 years
Technology Updates	Biometric for identity security such as heart-pulse rate measurement, electrocardiogram sensor, blood oximetry and skin temperature.	AI-based cybersecurity to learn about pattern recognition techniques, to capture the unstructured data and identify treats, building instincts and expertise	Quantum cryptography to encrypt information at the physical network layer
Potential Growth in Thailand	Smart Living and Smart City, Info Security and AI surveillance system initiatives by the Thai policy makers will drive the need on biometric identification, smart sensors and alarms and access control systems.	Thailand will start to apply AI on network traffic monitoring and Big Data Analysis to detect suspicious user behaviors	Quantum cryptography has become very attractive among Thai scientists due to its effectiveness to provide secret computational communication
Other Cybersecurity Technologies	• **Multifactor Authentication:** the authorization system that require more than one identification. Thai market is most familiar with this system through the uses of the recent iPhone models. • **Fingerprint sensor:** it is projected that many buildings in Thailand would implement fingerprint and facial sensor within 2020 as part of facility management initiatives especially in oil & gas sectors and banking. • **Eye printing:** This type of authentication is simple to use and is also in trend with new-age digital banks. The growing adoption of Artificial Intelligence (AI), virtual reality (VR), and augmented reality (AR) in consumer electronics & other commercial application will booze up the attraction for Eye Printing application over the coming year. • Vein Recognition: Vein recognition systems are the newest biometric technologies that have emerged in financial services. The technology uses vascular patterns of an individual's palm/finger for the personal identification of data. With its unique access control to authentication, this could be potential for properties and building security in Thailand.		

recovery time. For threats to the individual in Thailand, call-center scammers based in other countries are the country's most-reported cybercriminals. These hackers have incurred millions of baht in damage in recent years, duping Thai victims via Voice over Internet Protocol (VoIP).

Future Trend

Thailand's cybersecurity technologies and industry infrastructure are not yet at the mature stage, and they still struggle to secure the national security, digital facilities, online privacy, identity, integrity and digital transactions from cyberattacks. The highlights of Thailand's Cybersecurity in the next 15 years are:

Highlight of Potential Service and Platform for Cybersecurity in Thailand

Theft is the latest in a series of high-profile cybercrimes in Thailand in recent years, including a ransomware attack on Saraburi Hospital, Phetchabun Hospital, Krung Thai Bank, Lazada, Bangkok Airways, Centara Hotel Group, CP Freshmart (retail business of CP Group) and Bhumirajanagarindra Kidney Institute Hospital.

The specific cybersecurity technologies and platform that Thailand are lacking, and they will be in high demand by the local Thai businesses as follows:

- Zero Trust Dongles
- Single strong source of user identity
- User authentication (2FA)
- Machine authentication
- Compliance and device health
- Authorization policies to access an application
- Access control policies
- AIoT (AI can counteract cybercrime by identifying patterns of behavior on every IoT device)
- Cloud Breach

A good local Thai partner can enhance and personalize marketing efforts within market, and can help search for new projects and business opportunities on behalf of the foreign companies. Moreover, Thai buyers value relationships when dealing with sellers. The oversea companies are advised to utilizing the and developing relationships with local distributors or buyers in order to access into the Thai market.

Yada Saraneeyatham,
Senior Research Analyst - yada.s@tractus-asia.com

Tractus has been assisting companies in making informed decisions about where to invest and how to enter markets and expand their business in Asia and beyond for over 25 years. Whether you need an upfront market opportunity assessment and financial feasibility of your business model, a strategy for investing in markets or execution assistance to identify optimal sites for manufacturing and service operations or to identify the best joint venture partners or acquisition candidate, Tractus can help you develop an informed strategy and assist in its execution. For more information, visit www.tractus-asia.com