InterRisk Thai Report <2022 No.01>

Cybercrime in Thailand

[Summary]

- The users in Thailand were attacked by cybercrimes around 21% in 2021 which is lower than the global average of 29%.
- The average losses of cybercrime in 2021 rise up to 144%, or $2.2 million or approximately 72.6 million Thai Baht.
- Subsidiary companies are used as an intermediate for intrusion into the headquarters system.
- Regular training by specialists for quick communication in case of an accident is required.

Cybercrime is a crime that involves a computer and a network to further illegal ends, such as committing fraud, stealing identities, or violating privacy. Computer viruses are one of the cybercrimes; probably the first kind of crime you became aware of. Viruses infect computer systems, destroying files, messing with the overall functionality, and self-replicating to other devices and systems. Viruses are a form of malware, which encompasses all kinds of malicious software, any code or programs written and distributed to damage, steal data, and make money for the virus's owner. This includes ransomware, which can lock up your files until you pay a ransom to decrypt them.

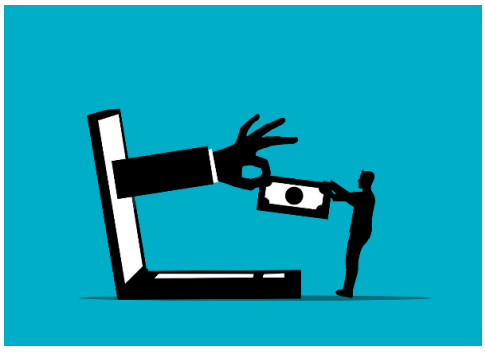
Cybercrime is a problem nowadays because technology is advancing every day. However, security measures to protect this technology and the users of the technology are not advancing as quickly. This allows for cybercrime to occur more often.

Cybersecurity Ventures, the world's leading researcher expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, which is exponentially larger than the damage inflicted from natural disasters in a year.

So, what are the cybercrime situation in Thailand? Let's find out the interesting information in this newsletter. In Thailand, the cybercrime incidents are divided into 9 categories as follows;

Table.1 Categories of cybercrime in Thailand

Type	Description
1. Abusive Content	Threats arising from the use and dissemination of abusive content to damage the reliability of individuals or institutions to cause conflict or illegal information such as pornography, defamation, and advertising of various products by email that the recipient does not intend to receive advertising information (SPAM)
2. Availability	Threats arising from attacks on the system, making the system unable to normally use. It affects service response or system failure. Threats may arise from service attacks directly, such as DOS (Denial of Service) attacks, or attacks on infrastructure that supports the services system such as buildings, power systems, and air conditioning systems.
3. Fraud	Threats arising from fraud can be happened in many cases, such as unauthorized using of systems or information for own benefit, creating a fake website page (phishing) that steals user's login passwords, or selling products or software that violate copyright
4. Information gathering	Threats arising from an attempt to collect information about the vulnerability of an attacker (Scanning) by using services that are available on the system such as operating system information, installed software information, account information, etc. This information includes collecting or checking traffic information on the network (Sniffing) to trick users to reveal important information of the system.
5. Information security	Threats arising from unauthorized accessing of sensitive information or unauthorized modifying of the information.
6. Intrusion Attempts	Threats arising from intrusion attempts, either through common vulnerabilities and exposures (CVE) or through uncommon vulnerabilities. Threats include attempts to hack the system, guessing methods of account authentication, username and login password, or testing every password (Brute Force)
7. Intrusions	Threats to systems that have been successfully intruded, resulting the system is occupied by unauthorized persons.
8. Malicious code	Threats arising from programs or software that have undesired results with the user or the system (Malicious Code), causing malfunction or damage to the system. Generally, this malicious program or software requires user to open the program or software. Therefore, they can install themselves and run them like Virus, Worm, Trojan or Spyware.
9. Other	Types of threats other than all of above. It is identified as new or unclassified threats. If the number of other threats is greater, this table need to revise the classification of the threat.



The trend of historical statistics of cybercrime incidents in Thailand since 2018 is decreased but the number of incidents is still high. The average losses of cybercrime in 2021 rise up to 144%, or $2.2 million. or approximately 72.6 million Thai Baht. The most affected industries were legal services, construction, wholesale and retail, healthcare, and industrial estates. Thailand is in 6th ranked in the Asia-Pacific countries and Japan is mostly affected by ransomware. According to the survey questionnaire of cyber companies in many countries, it was found that the users in Thailand were attacked by cybercrimes around 21% in 2021 which is lower than the global average of 29%.

In the last 4 years, the numbers of cybercrimes are 2,250 cases (in 2018), 2,470 cases (in 2019), 2,250 cases (in 2020), and 2,069 cases (in 2021) which have no significant changes. However, the incident type of intrusions was decreased while malicious code and other threats (such as information gathering) were increased. The situation of cybercrimes in Thailand in the last 4 years is shown as the following diagram.

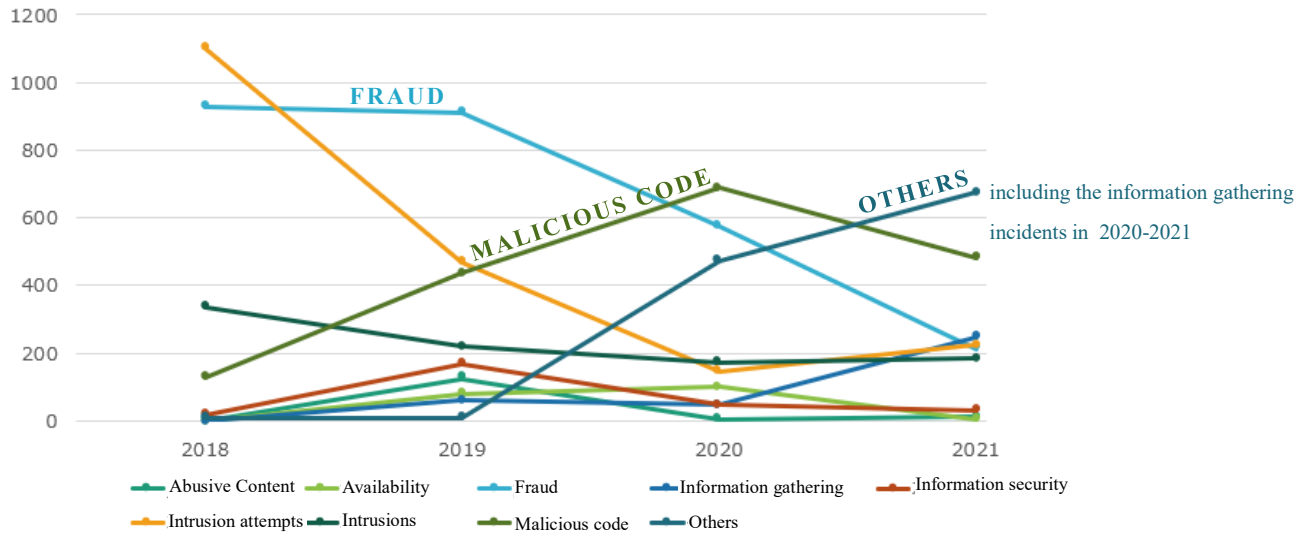


Figure.1 Number of cyber attacks in Thailand (2018 – 2021)

Examples of big cybercrimes in Thailand are shown in the below table.

Table.2 Examples of major cybercrimes in Thailand

Dates of accidents	Occupancies	Descriptions
August 2016	Bank	An automated teller machine (ATM) was attacked by malware, causing the loss of money of around 12 million Baht. The criminal withdrew 40,000 Baht each time from 21 ATMs, a total of 300 withdrawal times.
July 2017	Bank	Three thousand company names that provide an online letter of guarantee were leaked. Moreover, there is a case from the other bank that 120,000 data accounts were leaked from online requests for microloans such as housing loans and personal loans.
March 2018	Communication company	Almost 11,400 clients' data was leaked from a big communication company.
May 2020	Communication company	More than 8,000 million lists of internet logs were leaked from the biggest communication company. According to the company's report, the leaked records are only represented the overall internet log and it does not show personal data or customers' confidential data.
September 2020	Hospital	The hackers attacked the hospital's system with a ransomware. The entire systems were inoperable and disrupting medical services. The criminal demanded 200,000 Bitcoins (about 63 billion Baht).
May 2021	Insurance company	The big insurance group was targeted in the cybercrime by the "Avaddon" hacker group. The data size of 3 TB including clients' medical reports (sensitive information), scanning documents of bank accounts, and identification cards were leaked.

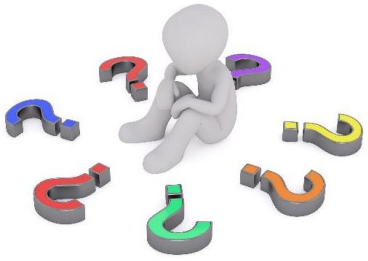
The principle of cybersecurity measures

Due to the limited resources (people, time, and budget) of the foreign subsidiaries compared with the headquarters, the security level of foreign subsidiaries therefore tends to be lower than the headquarters. The attackers have already known this condition. Thus, the attack of foreign subsidiaries will be an intermediate for intrusion into the headquarters system.

There are various types of cyberattacks in the past year, causing the high flexibility to deal with the situation is required. Although the details of the countermeasure have already been known, the proper handle cannot be guaranteed. Since independent coping with the situation after the accident without the support from specialists is difficult, the segregation of responsibilities among foreign subsidiaries, headquarters, and external cybersecurity specialists is obviously important. In this article, regular training is suggested to prepare the countermeasures starting from the anomaly detection to initial responses through concrete simulation situations as the examples below.

From detection to initial response

"Did you notice?" (Anomaly detection)	Can you observe and be aware of cyberattacks abruptly and minimize the damage? (Employees have been trained and provided the information ever since under normal circumstances. The results are recorded in a document format.)
"Can you report and start taking action yourself?" (Initial response)	Sharing all information ▪ Who does the first witness have to consult or report? *What should the basic countermeasure be referred to? ▪ Who is responsible for cyberattack judging (or possibly being a cyberattack) and taking responsibility to provide the countermeasure subsequently? ▪ Is it necessary to report to a mandated person? *Are there any penalties if the suspected cases were not reported? Reporting to headquarters ▪ Are the reporting procedures to headquarters and the emergency contact clear? *If the malware infection or data leakage has been confirmed, the report to headquarters should be performed immediately, especially if the network is connected to headquarters, resulting in the increase of damages which can possibly occur to headquarters. Restriction, investigation, and analysis ▪ Are the following items clear; the contact information of the mandated department staff and the external cybersecurity specialists, the coordination and communication system, and the segregation of responsibilities? *Due to the difficulty of making decisions and coping with the situation in your company or headquarters, communication with the cybersecurity experts is highly necessary, especially in the initial response process.



Supporting the system recovery through the insurance and additional services.

This section mentions cybersecurity insurance. In the event of cyber incidents as shown in the table on page 3, your company's initial response is very important to mitigate losses. Besides a quick response, an advanced technical countermeasure is also necessary. There are very few foreign subsidiaries with limited resources that can independently cope with cyber incidents without supporting from external organizations. Therefore, regular training and preparation of emergency communications are required for swift communication with cybersecurity specialists in case of an accident.

If the insurance on cyber security has been covered on your company already, the insurance company will contact cybercrime specialists and immediately troubleshoot to recover as soon as possible. If the emergency communication with contracted IT companies has been proceeded, problems will be solved faster as well. In addition, there are insurance companies that provide training services such as phishing email training which can increase the efficiency of cybercrime response. The example of training is shown in the below figure.

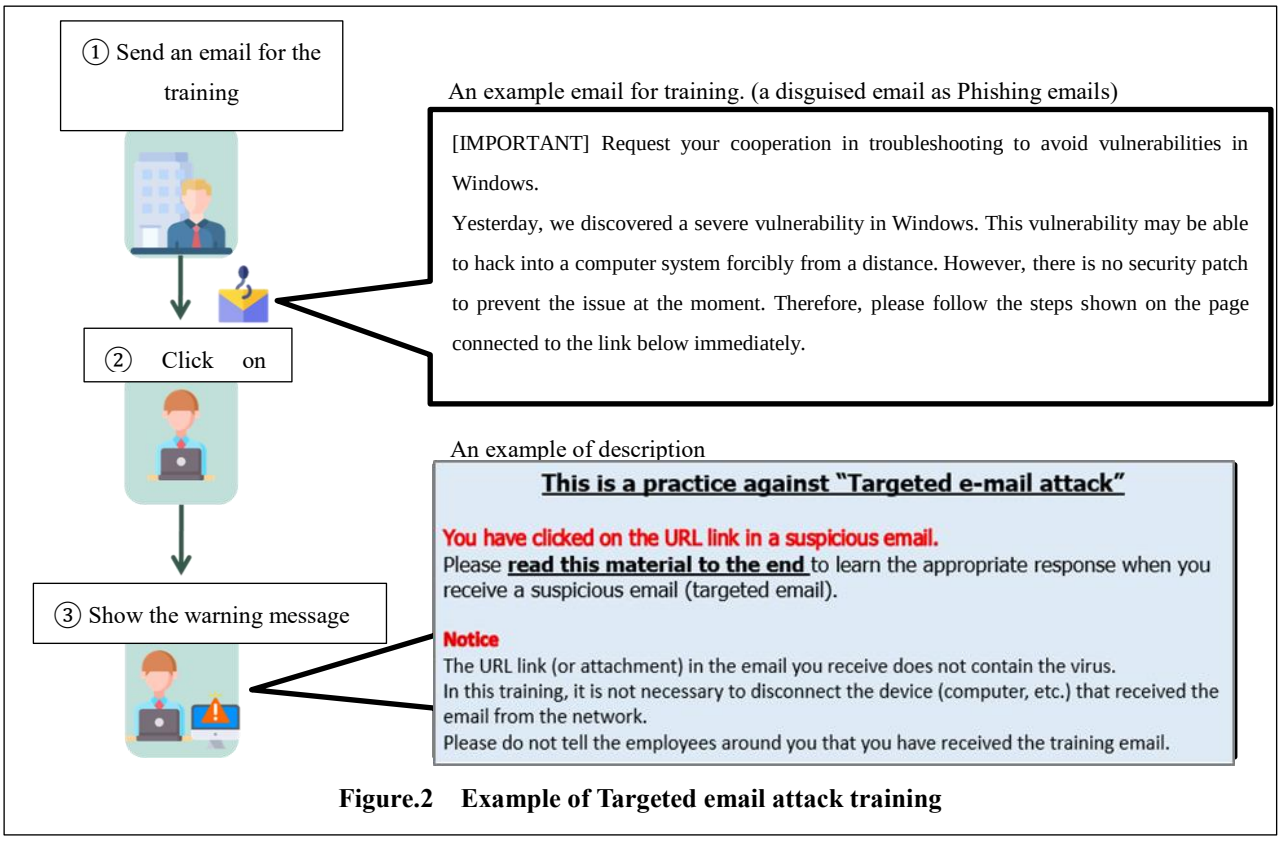


Figure.2 Example of Targeted email attack training

The cyber risks such as the enormous financial burden caused by ransomware damage are increasing and more complicated every year. Besides direct damage from cybercrimes, the number of consequential damages and minor incidents is also increasing. Such situations do not affect only your company, it also affects business partners, customers, and shareholders. In some cases, it may affect the market and society as well. Therefore, please be informed that the situation can be resolved with urgency and advanced technical response even in a limited resource condition if insurance services are utilized effectively.
The benefits of using insurance services are as follows:

1. Encouragement of cyber-attack training and provision of training equipment about phishing email training for employees etc.
2. Support of emergency measures and system restoration with coordinated specialists in case of cyber incidents.
3. Reimbursement of recovery cost of post-cyber-attacks, losses incurred with stakeholders (such as business partners, etc.), expenses incurred in emergency measures, compensation cost for victims in case of the personal data leak, and compensation cost for business partners in case of confidential information leak, etc.

References

- https://www.avast.com/c-cybercrime
- https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx
- Kaspersky Security Bulletin Overall Statistics for 2020
- https://www.itday.in.th/kaspersky-reveals-a-30-45-percent-increase-in-web-threats-targeting-thai-users-in-q1-64/
- https://www.newsdirectory3.com/top-5-cyber-threats-to-attack-asean-thai-big-target-and-ransomware-that-hopes-more-than-money/
- https://www.terranovasecurity.com/what-is-ransomware/
- https://www.thairath.co.th/news/tech/2375175
- https://www.trendmicro.com/vinfo/us/security/definition/ransomware

Source of image

- https://www.pixabay.com/photos/hacker-silhouette-hack-anonymous-3342696/
- https://www.pixabay.com/photos/regulation-gdpr-data-protection-3246979/
- https://www.pixabay.com/illustrations/question-mark-think-question-2318030/
- https://www.pixabay.com/vectors/scam-phishing-fraud-money-6922102/

MS&AD InterRisk Research & Consulting, Inc. is a MS&AD Insurance Group company specialized in risk management survey research and consulting services. For inquiry about consultation and seminar etc. for companies expanding business in Thailand, please feel free to contact the nearest Mitsui Sumitomo Insurance or Aioi Nissay Dowa Insurance sales representatives.

MS&AD InterRisk Research & Consulting, Inc.
International Section, Corporate Planning Department
TEL.03-5296-8920
http://www.irric.co.jp

InterRisk Asia (Thailand) is a MS&AD Insurance Group company which was established in Thailand to provide risk management services, such as fire safety, flood risk management, electrical safety and risk consulting services, such as automotive risk assessment, occupational safety and burglary risk survey to our clients in Thailand. For inquiry, please feel free to contact us.

InterRisk Asia (Thailand) Co., Ltd.
175 Sathorn City Tower, South Sathorn Road, Thungmahamek, Sathorn, Bangkok, 10120, Thailand
TEL: +66-(0)-2679-5276
FAX: +66-(0)-2679-5278
http://www.interriskthai.co.th/