TOKIO MARINE
INSURANCE GROUP

Cyber Insurance

19th Feb. 2019

Tokio Marine Asia

tokiomarine.com
Life & Health| Property & Casualty

Cyber Risk and Cyber Insurance

1. What is Cyber about?
2. How to tackle Cyber Risks?
3. How Cyber Insurance Protect your business?
4. Updates of PDPA (Personal Data Protection Act) in Singapore
5. Claim Services for the Cyber Incident
6. Product Summery

So what is Cyber about?

CyberSecurity Malaysia, an agency under the Science, Technology and Innovation Ministry, has urged Internet users to be cautious with their machines

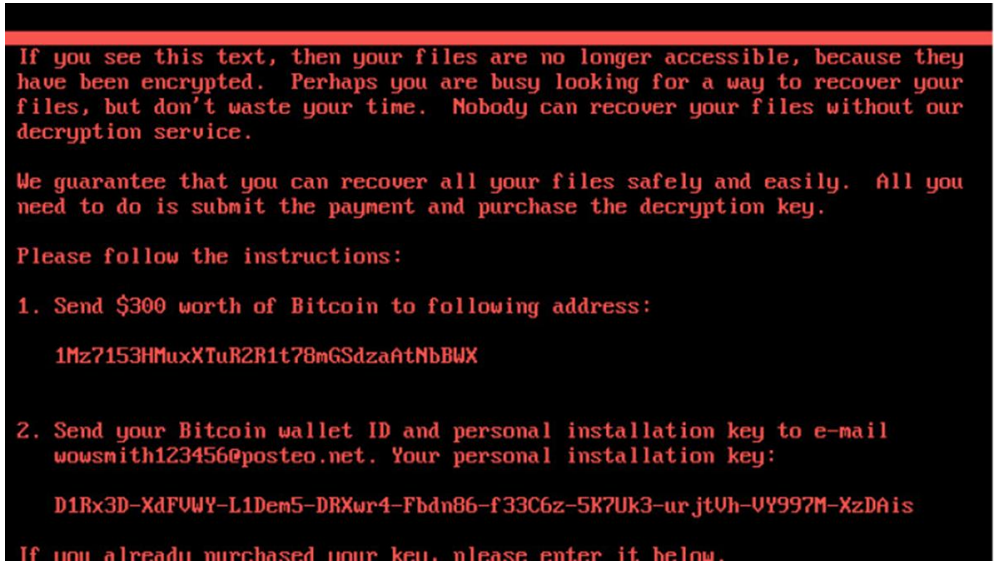
The attack, which locks computers and holds users' files for ransom, hit **200,000 victims in 150 countries** over the weekend.

The massive attack shut down work at 16 hospitals across the United Kingdom. Car manufacturers like Nissan and Renault halted their production in several of their factories across the UK.

Other organisations hit include the Swedish engineering firm Sandvik, the German train operator Deutsche Bahn, FedEx, the Russian Interior Ministry and several global telecoms companies.

Most recently, Malaysia and Singapore have been added to the growing list of countries hit by the attack.

A digital directory service at Tiong Bahru Plaza in Singapore was affected by the WannaCry virus over the weekend.



Experts says Petya's threats are more powerful than WannaCry. Once the computer compromised by the virus, there would be the possibility that stored data shall be damaged completely.

On 27 June 2017, a major global cyber attack began (Ukrainian companies were among the first to state they were being attacked), utilizing a new variant of Petya.

On that day, Kaspersky Lab reported infections in France, Germany, Italy, Poland, the United Kingdom, and the United States, but that the majority of infections targeted Russia and Ukraine, where more than 80 companies initially were attacked, including the National Bank of Ukraine. ESET (IT company in Ukraine) estimated on 28 June 2017 that 80% of all infections were in Ukraine, with Germany second hardest hit with about 9%. Russian president Valdimir Putin's press secretary, Dmitry Peskov, stated that the attack had caused no serious damage in Russia. Experts believed this was a politically-motivated attack against Ukraine, since it occurred on the eve of the Ukrainian holiday Constitution Day.

- **Shipping Giant, Maersk and Goods Delivery Company, Fedex, both company have announced their losses would be more than USD300 m in revenue caused by Business Interruption by malware infection**
- **Pharmaceutical Giant, Merk also suffer Business Interruption by Petya/Not Petya attack, along with Cadbury (confectionary), DLP Piper (lawfirm) and Mondelez International (Oreo-maker).**

China's Secret Weapon in the South China Sea: Cyber Attacks

After the South China Sea ruling, China throws another digital tantrum.

The Diplomat - July 22, 2016

Despite China's great power aspirations, its cyber warriors threw a fit after losing a legal battle to the Philippines in The Hague. Within hours of the Permanent Court of Arbitration's unanimous rebuke of China's territorial claims in the South China Sea last week, at least **68 national and local government websites in the Philippines** were knocked offline in a massive distributed denial of service (DDoS) attack.

More than 100 flight delayed due to cyber-attacks at Vietnam's airports

Thanh Nien News Saturday, July 30, 2016 14:00

The cyber-attacks on Vietnam's two major airports have affected more than 100 flights, dozens of which were delayed for up to one hour, the country's aviation authorities said.

The Civil Aviation Authority of Vietnam (CAAV) said in a press release Saturday that it has ordered other airports across Vietnam to tighten aviation security after hackers targeted computers systems at the airports in Hanoi and Ho Chi Minh City.

The computer systems at Tan Son Nhat airport in Ho Chi Minh City were hacked at 1.46 p.m., and Hanoi's Noi Bai airport at 4.07 p.m..

The hackers, allegedly from China, took control of the flight information screens and displayed distorted information about the East Sea (South China Sea) and insulted Vietnam and the Philippines, according to authorities.

The personal details of some **46.2 million mobile phone subscribers** in Malaysia have been stolen, in what is believed to be the largest data breach in the country, local media reported on Dec. 31, 2017 (Strait Times Nov. 1, 2017)

Online technology site lowyat.net said the hackers have the home addresses, identity card numbers, SIM card information and private details of almost the entire Malaysian population of 32 million. Many Malaysians have several mobile numbers.

In addition, 81,309 records from the Malaysian Medical Council, the Malaysian Medical Association and the Malaysian Dental Association were also exposed, the tech site said.

Communications and Internet regulator, the Malaysian Communications and Multimedia Commission (MCMC), has said it is investigating the breach with the police.

The Biggest Data Breaches in the ASEAN Region (Resource – CIO Asia (magazine))

Philippines (Jan 2019): Cebuana's marketing server breached

Cebuana is the leading and largest non-banking financial services firm.

900,000 of their clients' information, including date of birth, address, source of income were compromised.

Internal investigation found that data was stolen in August 2018.

Cebuana had reported the breach to the National Privacy Commission and the commissioner started official investigation.

WORLD ECONOMIC FORUM 2019 Global Risk Report has named ***Cyber Attacks*** *and* ***Data Breaches*** *as he* ***FOURTH and FIFTH*** *most serious risks facing the world today.*

The Biggest Data Breaches in the ASEAN Region (Resource – CIO Asia (magazine))

Singapore (Jan. 2019): Second Health Data Breach in Six Months

Confidential information belonging to 14,200 people diagnosed with HIV was stolen and leaked online in Singapore.

Ministry of Health published statements the information included names, contact details, HIV test results and other medical information.

MOH believes the leak was committed by a US citizen lived in Singapore.

This person used to be the partner of the former head of Singapore's National Public Health Unit.

MOH stated 'access to the confidential information has bee disabled, but it is still in the possession of the unauthorized person.

Singapore (July, 2018): Largest Data Breach

SingHealth's 1.5 million patients including the Prime Minister Lee Hsien Loon and several ministers information were stolen. The information included names, National Registration Identity Card numbers, address, dates of birth.

A committee of inquiry (COI) investigate the incident in October and finished on 30 Nov. Found the fact that Integrated Health Information System (IHiS), the agency which runs IT systems terminated the SingHealth's electronic medical records system intrusion began on June 27 2018 but only discovered on July 4, 2018. It took SIX days since the attack began to be discovered.

IHis staff initially thought that no data had been stolen.

The Biggest Data Breaches in the ASEAN Region (Resource – CIO Asia (magazine))

Philippines May 2018: Jollibee Food Corporation (JFC)

National Privacy Commission of Philippines gave 10 days order to Jollibee Food Corporation (JFC) to come up with a plan to rehabilitate the vulnerabilities in its website, which could expose the data of millions of customers in the case of a breach. In addition to that the authority ordered JFC to employ privacy by design in re-engineering JFC's data infrastructure. JFC need to conduct a new privacy assessment and filing monthly report to the authority

Philippines May 2018: Wendy's

US-fast food chain with operations in the Philippines had data breach of 82,150 records of customers and job applicants including names, addresses, passwords, payment methods and transaction details were compromised to leak.

National Privacy Commission of Philippines ordered Wendy's to inform users affected by the data breach within **72-hours**. The authority stated on an analysis of the information compromised, it can be ascertained that the exposure of certain sensitive personal or financial information within the database puts the affected data subjects in harmful way'.

The Biggest Data Breaches in the ASEAN Region (Resource – CIO Asia (magazine))

Thailand (March 2018): True Corp

Researcher Niall Merrigan found the identity documents of 45,736 customers of True Corp had been exposed.

All these personal information were belonged to customers of True Corp's e-commerce subsidiary iTrueMart (now WeMall) and stored in a public-facing Amazon S3 bucket.

The data consisting mainly of JPG and PDF scans of identity documents including scanned ID cards driving licenses and possibly passports.

It was said that True Corp was wrongly assuming the incident was a hack but there was no security on the Amazon S3 data bucket and anybody could found and download the files.

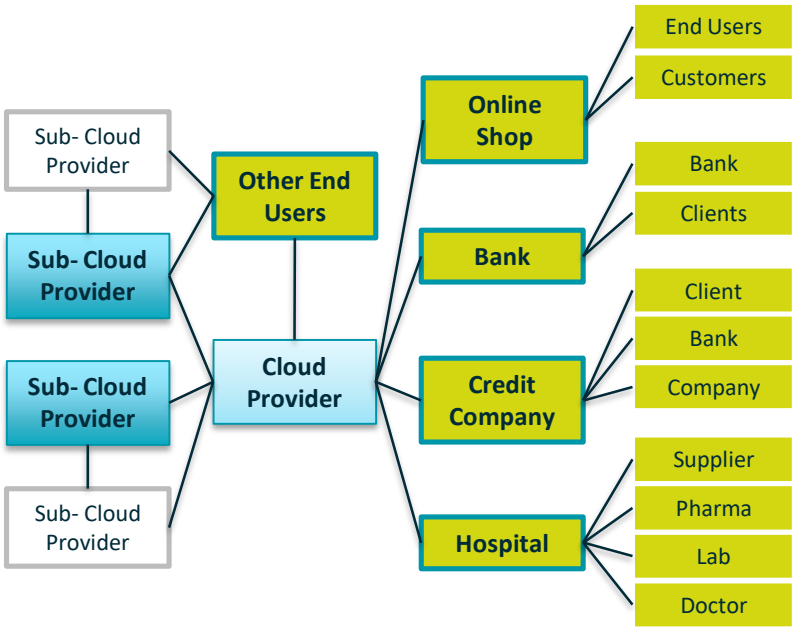
Bangkok Post said Telecoms regulator NBTC is investing the incident and may force True Corp compensate its customers for exposing their details. The data was collected as part of the Thai government's mandatory SIM registration scheme, which has already been a target of identity thieves and has been opposed by privacy advocates.

It is not clarified yet that whether True Corp had to have intentionally set the data to public as Amazon S3 services could be private setting.

Today's Cyber Risk Environment

> Globally

- There is growing focus on data, technology and interconnectivity
- Companies are collecting, storing and processing large amount of data
- Our reliance on the internet and computer systems is growing exponentially:
  - Mobile Apps/Mobile Business
  - Automated systems
  - Social Media Usage
  - Cloud computing
- Increase use of technology leads to increase exposure to cybercrime attacks

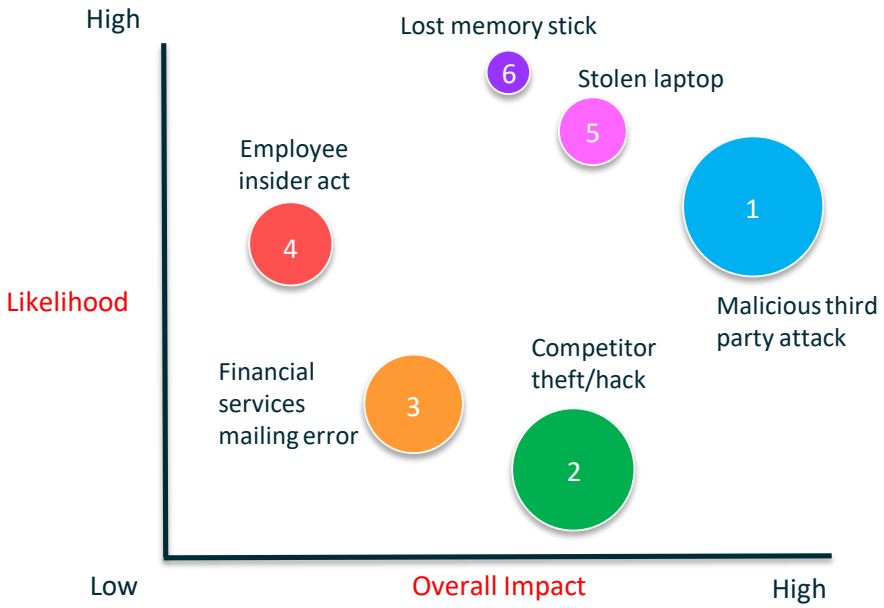


Types of Cyber Perils

> Exposures can be from anywhere on any day

- Hacking of the computer or network
- Virus / malware
- Employee sabotage
- Employee error
  - ➢ Accidental deletion
  - ➢ Accidental mail sent to wrong recipient
- Lost or misplaced company files and/or laptops, mobiles, thumb drives

Cyber attackers are continuously discovering new ways to exploit vulnerabilities, cyber security alone cannot prevent all potential attacks.



How to tackle Cyber Risks?

Manage and Control of IT Digital Assets of the Company

Use the latest updated version of Application Software

Experts found that WannayCry case, the malware attacked to the Microsoft's software such as Windows XP or Windows Server 2003 which have been out of supporting period. This means the latest security batch services would be finished. The company may be strongly recommended to use the updated version to get support from the software provide in regular basis.

Restriction or Prohibit usage of Pirate and/or Illegal Software or Device

In Asia, the experts have been warning on significant usage of pirate or illegal software downloads and usages. The problem is not only the breach of copy rights, but these pirate or illegal software may cause the huge damage to users' computer system as these might be already infected by malwares. There are many cases have been seen that an employee's personal USB memory spreads the malware when the employee insert his/her USB memory to the company's PC and company's server and networks are infected instantly. Then the company's server may be compromised which is led to leak the data stored in the server.

Network Management

Restriction/Control/Limitation of Accessibility of NETWORK SYSTEM

Aside from updating of the latest Software, installing appropriate Anti-Virus software, another prevention method would be introduce the internal rules to limit accessibility of employees to the E-mail or Website. For example, to limit the E-mail access only to internal mail server system or to introduce the access block system for certain websites where irrelevant to the businesses. Even some file exchange software, such as Drop Box, these are open resource over the internet may be prohibit the employees to use for business purposes. These free software may be considered to have very weak security protections.
And if it is necessary, any confidential information for the company (design drawings, formula for the chemical products, etc.) would be not stored in any PC/server which is connected to the network but securely store them under off-line computer, etc.

Regular Trainings against Social Engineering Attacks

Nowadays, more and more Social Engineering Attacks are getting seen in many countries. And these attacks are getting more trickier and looking genuine. It is getting very difficult to figure out which is fraudulent or not. It requires regular and continuous training to employees to encourage their sense to feel something not quite right about the mail. 。

Post Incident Control Plan

Although the company may well prepare and maintain the security systems to protect their PC/Server/Network System, the level of Cyber Attacks never stand still, always advanced. This means it is almost impossible to achieve 100% protection against Cyber Attacks. It is highly recommended to prepare and maintain the protocols/ procedure for the post incident. In order to protect the company's brand image, it is important to how to handle the public reputations, such as announcement by the company to affected parties, etc.

Loss Amount Estimation and Control

It is also strongly recommended to estimate the amount of losses incurred by the incident caused by Cyber Attacks. Maximum losses estimated by the shut down of computer systems. Along with loss of income during the outage of the computer system, there would be also needed to consider the costs and expenses to investigate the cases and restoration of the computer system.

Personal Data Protection Act (2012) in Singapore

A Quick Guide to the PDPA 2012 for Organizations

Personal Data

Refers to data, about an individual who can be identified from that data, or from that data and other information to which an organization has or is likely to have access.

Range from names, contact numbers and addresses to other types of data that do not directly identify an individual on its own but form part of an accessible record about an individual.

ORGANIZATION

Subject to ALL the obligations under the PDPA.

(unless exception applies)

Data Intermediary

Subject to the Protection and Retention Limitation Obligations only, where it processes personal data for another organization under a written contract

A Quick Guide to the PDPA 2012 for Organizations

9 Obligations

1. Consent Obligation
2. Purpose Limitation Obligation
3. Notification Obligation
4. Access & Correction Obligation
5. Accuracy Obligation
6. Protection Obligation
7. Retention Limitation Obligation
8. Transfer Limitation Obligation
9. Openness Obligation

PERSONAL DATA PROTECTION COMMISION (PDPC)

Personal Data Protection Complaint Handling

When a complaint is received by the PDPC, the PDPC may assess if it can help to address the individual's concerns by facilitating communications between the individual and organisation.

If an individual and an organisation are unable to resolve the matter directly and require additional assistance, the PDPC may refer the matter for mediation by a qualified mediator.

If the matter is resolved amicably, the PDPC will generally not proceed with further investigations.
The PDPC encourages all parties to consider the above processes before lodging a complaint with the PDPC.

The PDPC may, upon complaint or of its own motion, conduct an investigation to determine whether an organisation is compliant with the PDPA.

PERSONAL DATA PROTECTION COMMISION (PDPC)

Power to Require the Production of Documents or Information

Where the PDPC has reasonable grounds for suspecting that an organisation is not complying with the PDPA, it may require any organisation to produce specified documents or to provide specified information, by written notice.

When requiring an organisation to produce a document, the PDPC may:

- **take copies or extracts from any document produced;**
- **require a person served with a notice to produce the document to provide an explanation of the document produced; and**
- **if the document is not produced, require a person served with a notice to produce the document (or any past or present officer or employee of that person) to state, to the best of that person's knowledge or belief, where the document can be found.**

PERSONAL DATA PROTECTION COMMISION (PDPC)

Power to Enter Premises for Inspection

The PDPC has powers enabling it to enter premises and to gain access to information, documents and equipment or articles relevant to an investigation.

Power to Enter Premises without Warrant

The PDPC may effect entry into any premises without a warrant by giving the occupier of the premises at least 2 working days' written notice of the intended entry and indicating the subject matter and purpose of the investigation.

The PDPC may also effect entry into any premises without a warrant and without notice, if the inspector has reasonable grounds for suspecting that the premises are, or have been, occupied by an organisation which is being investigated in relation to a contravention of the PDPA.

PERSONAL DATA PROTECTION COMMISION (PDPC)

Power to Enter Premises for Inspection

The PDPC has powers enabling it to enter premises and to gain access to information, documents and equipment or articles relevant to an investigation.

Power to Enter Premises without Warrant

The PDPC may effect entry into any premises without a warrant by giving the occupier of the premises at least 2 working days' written notice of the intended entry and indicating the subject matter and purpose of the investigation.

The PDPC may also effect entry into any premises without a warrant and without notice, if the inspector has reasonable grounds for suspecting that the premises are, or have been, occupied by an organisation which is being investigated in relation to a contravention of the PDPA.

PERSONAL DATA PROTECTION COMMISION (PDPC)

Directions to Secure Compliance

Section 29(1) of the PDPA provides that the PDPC may, if it is satisfied that an organisation is not complying with any of the Data Protection Provisions, give the organisation such directions as the PDPC thinks fit in the circumstances to ensure the organisation's compliance with that provision.

- to stop collecting, using or disclosing personal data in contravention of the PDPA;
- to destroy personal data collected in contravention of the PDPA;
- to comply with any direction of the PDPC under section 28(2) of the PDPA;
- to pay a financial penalty of such amount not exceeding $1 million as the PDPC thinks fit

PERSONAL DATA PROTECTION COMMISION (PDPC)

General Offences and Penalties

It is an offence under section 51(3)(b) and (c) of the PDPA to:

obstruct or impede the PDPC, its inspectors or other authorised officers in the exercise of their powers or performance of their duties under the PDPA; or

knowingly or recklessly make a false statement to the PDPC, or knowingly misleads or attempts to mislead the PDPC, in the course of the performance of the duties or powers of the PDPC under the PDPA.

An organisation or person that commits an offence under section 51(3)(b) or (c) of the PDPA is liable to:

- in the case of an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both; and
- in any other case, to a fine not exceeding $100,000

PERSONAL DATA PROTECTION COMMISION (PDPC)

22 Jan 2019: Breach of the Protection Obligation by COURTS

A financial penalty of $15,000 was imposed on COURTS for failing to put in place reasonable security arrangements to protect the personal data of its customers from unauthorised disclosure on its online portal.

15 Jan 2019: Breach of the Protection Obligation by SingHealth and IHiS

Breach of the Protection Obligation by SingHealth and IHiSA financial penalty of $250,000 and $750,000 was imposed on SingHealth and IHiS respectively for the failure to make reasonable security arrangements to protect personal data of individuals.

03 Jan 2019: Breach of the Protection Obligation by Toppan Forms

A financial penalty of $5,000 was imposed on Toppan Forms for failing to put in place reasonable security arrangements to protect the personal data from unauthorised disclosure.

03 Jan 2019: Breach of the Protection Obligation by Bud Cosmetics

A financial penalty of $11,000 was imposed on Bud Cosmetics for failing to put in place reasonable security arrangements to protect the personal data of its customers from unauthorised disclosure. Directions were also issued to the organisation to engage qualified personnel to conduct a security audit, develop an IT security policy, and implement a training policy.

How Cyber Insurance Protect your business?

The Cover…

Notification Costs

Computer Forensics

Third Party Liability

Regulatory Defence

Loss of Income

Data Restoration

Loss Scenario 1

Auto Parts Manufacturer

(Company profile)
Turn Over: USD100 million
# of Employees: 400

Cyber Incident
Company's computer systems which control the assembly lines of the factory has been infected by Ransom Ware.
As the company maintained Back Up System and recovery protocol, operation was fully resumed within 48 hours.

Estimated Losses incurred by the Company

- Operation Shut Down: 48 hours
- Income Loss: USD300,000
- IT Forensic/restoration Costs: USD100,000

There would be reputational damage (non-monetary loss), because of delay in deliveries to the clients.

Cyber Insurance Responses

Emergency Services at the time of Cyber Incident
24/7 Hot Line Services for initial consultation and advice

IT Forensic/Investigation Costs and Restoration Costs
After consultation by 24/7 Hot Line services, it is still requires IT professional's physical attendance to the company's venue, the IT professionals under the list of our supporting panel will be sent out.
Insurance Policy shall pay costs and expenses incurred by the IT professional's Forensic and Restoration services.

Business Interruption
The policy shall pay the Income Loss out of the operation shut down.

NOTE : All terms and conditions shall be fully depends upon the policy. There would be the case that exclusions shall be applied.

Loss Scenario 2

E-commerce

(Company Profile)
Turn Over: USD300
# of Employees: 800

Cyber Incident

A hacker conducted unauthorised access to the hacker to the company's Server, amended the website and place malware. Personal data of the users of the website has been stolen.

Estimated Losses incurred by the Company

- Website Shut Down: 10 days
- Income Loss: USD340,000
- IT Forensic/restoration Costs: USD150,000
- Extra costs for manpower: USD18,000

Potential decrease in sales as the web users may not come back after the incident.

Cyber Insurance Responses

Emergency Services at the time of Cyber Incident

24/7 Hot Line Services for initial consultation and advice

IT Forensic/Investigation Costs and Restoration Costs

After consultation by 24/7 Hot Line services, it is still requires IT professional's physical attendance to the company's venue, the IT professionals under the list of our supporting panel will be sent out.

Insurance Policy shall pay costs and expenses incurred by the IT professional's Forensic and Restoration services.

Business Interruption

The policy shall pay the Income Loss out of the Website shut down. Plus extra manpower to maintain the operations.

NOTE : All terms and conditions shall be fully depends upon the policy. There would be the case that exclusions shall be applied.

Cyber Insurance Responses

Personal Data leakage might be triggered to further losses incurred by the Company

1）Investigation by the Authority

Although the personal Data Protection Act or any similar regulations are not enforced in Thailand yet, there would be the case that Authority may conduct investigation for the causes of data leakage or any further actions may be taken.

The policy shall pay for costs and expenses to deal with the investigations by the Authority – IT forensic and any reports for the results, lawyer's fees, etc.

2）Notification Costs

If the Authority may order to the company for notification to affected persons regarding to the leakage, then the policy shall pay the costs and expenses for such notifications.

NOTE : All terms and conditions shall be fully depends upon the policy. There would be the case that exclusions shall be applied.

Real Case in Singapore

Company: Facility Management for Commercial Complex Building
Turnover: SGD100 m
# of Employees: 50

Incident 1 (RANSOMWARE)
Ransomware incident in March 2018. Some of the files in the on-premise file server was affected by ransomware due to the insufficient anti-virus agent installation.

Emergency IT on-site services: **SGD10 K**

- Removing viruses
- Restoring data back from the backup
- Detecting the cause of Incident
- Full virus scanning on PCs and servers

NOTE : All terms and conditions shall be fully depends upon the policy. There would be the case that exclusions shall be applied.

Real Case in Singapore

Company: Facility Management for Commercial Complex Building
Turnover: SGD100 m
# of Employees: 50

Incident 2 (E-MAIL HACKING)
E-mail hacking incident in August 2018. One of the staff's office 365 credentials were compromised due to accessing the URL link in a spam mail and the login attempt.

Emergency IT on-site services: **SGD130 K**

- Analysis of hacked account (checking log of Officer365) SGD9 K
- Analysis of all staff's account (confirming the extent of the hacking) SGD69 K
- Analysis of hacked account (checking hacker's activities during the hacked period via e-mail send/receive log) SGD18 K
- Analysis of URL access log (checking the cause of the credential compromised) S$35 K

NOTE : All terms and conditions shall be fully depends upon the policy. There would be the case that exclusions shall be applied.

Coverage Summary

What We Cover		Description
Third Party	Security and privacy liability	Liability and claims expenses incurred, arising from a security breach or privacy breach by the company, outsourcers or independent contractors
First Party	Privacy regulatory defense and Penalties	Resulting from civil regulatory action, caused by a privacy breach or breach of privacy regulations
	Crisis Management Event costs	Legal costs to comply with privacy regulations, credit monitoring, PR, legally required notification costs, resulting from a security data breach, privacy breach or breach of privacy regulations
	Cyber Extortion	Extortion expenses and monies paid resulting from a threat to destroy or release a company's digital assets which are acquired by unauthorized access
	Loss of Digital Assets	Expenses & costs incurred resulting from damage, alteration, theft, destruction of the company's digital assets caused by DOS, malicious code, unauthorized access/use to computer system
	Business Interruption Expenses	Income loss and extra expense resulting from a total or partial failure of the computer system caused by DOS, malicious code, unauthorized access/use to computer system

Major Exclusions

Typical Exclusions

- Retroactive Date (Excl 1)
  - No cover for events/circumstances/viruses that happened before the retroactive date
- Inception Date (Excl 2)
  - No cover for claim or any acts, facts, or circumstances that happened before the inception date, if the Insured knew or could have reasonably foreseen
- Bodily Injury (Excl 8)
- Property Damage (Excl 9)
  - No cover for hardware, but restorage expense for data and computer programs that exists in computer system is covered
- Failure in power, telecommunications other infrastructure (Excl 10)
  - No cover for infrastructure failure unless under the Insured's operational control
- NAT CAT or any other physical event (Excl 14)

Major Exclusions

Typical Exclusions

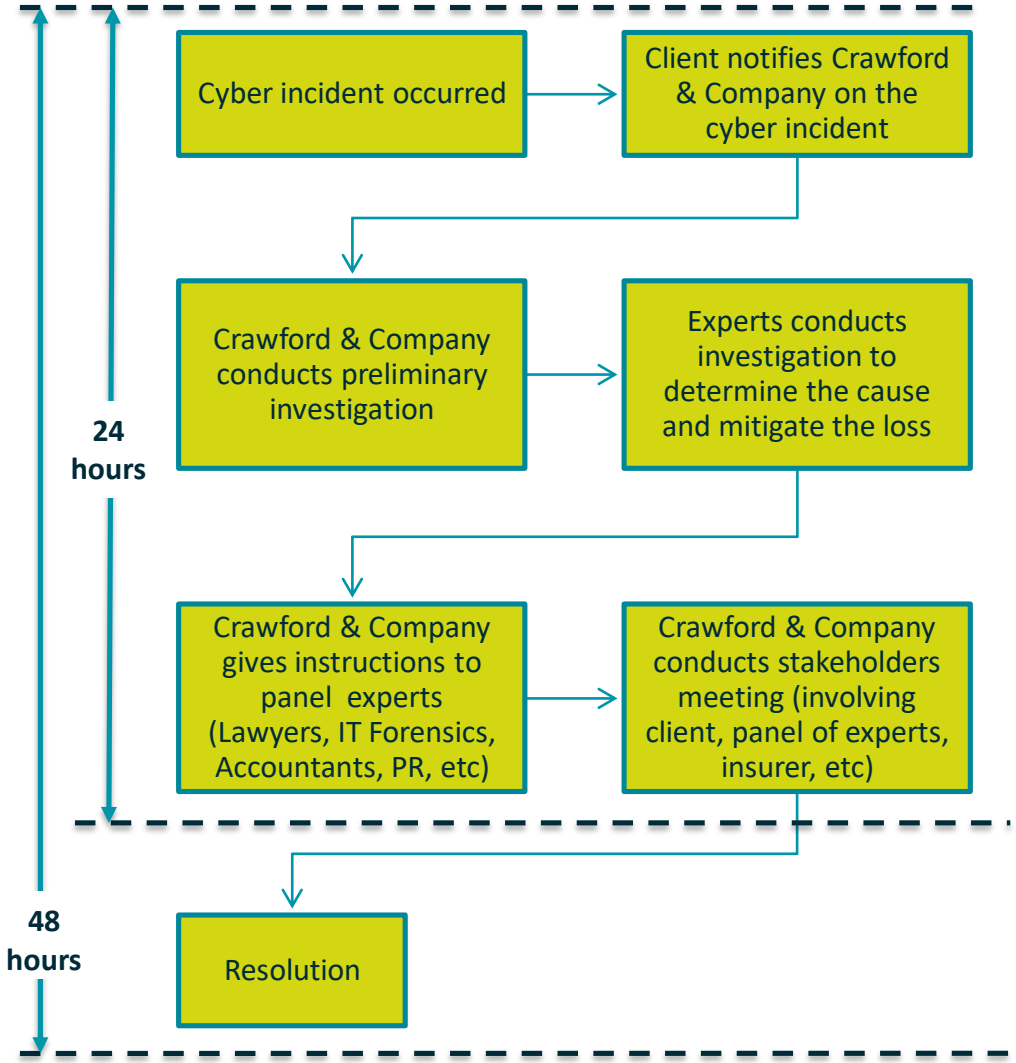
- Act of Terrorism, war, invasion (Excl 30)
  - No cover for Terrorism, war, invasion, but Act of cyber terrorism (Electronic, digital threat of any person or group, whether acting alone or in connection with any organization or government) is covered
- Fine or Penalty arising out of Payment Card Industry Standard/Payment Card Company Rules (Excl 33)
- Infringement of any patent or trade secret by Insured, Insured former employee (Excl35)
- Unlawful collection of personally identifiable non public information by Insured (Excl 43)
- Theft, Loss of unencrypted Lap tops and mobiles (Excl 44)

24/7 Hot Line Claim Services for your assistance!

Our Cyber Insurance Product

> Crisis Management and Support

- SPEED and EXPERTISE are essential in cyber crisis management to identify the root cause of loss and mitigate the loss within the quickest possible time.
- We, Tokio Marine, appointed Crawford & Company, a leading global cyber crisis management expert, as a agent for Tokio Marine from initial notification through to resolution, 24/7/365.
- We work with a dedicated breach response team with vast experience, which includes specialist lawyers, IT forensic investigators, forensic accountants and PR consultants, to ensure the best outcome for our clients.



So what TMiS can offer?

Our Cyber Insurance Product

Tokio Marine Group Cyber Insurance Product Strength

- Tokio Marine Group has more than 10 years' experience in providing cyber insurance. Our experience has allowed us to develop the most sophisticated Cyber insurance solution for our clients' needs.
- We cover business interruption losses due to malicious attack where our client's computer system or digital assets are handled by their named vendors
- Breach responses costs cover can be extended to voluntary notification costs
- Cover do not exclude Cyber Terrorism ➔ COMPETITOR'S WORDING CHECK!!
- Flexibility on choosing Limit from SGD500,000 to SGD10M
- Flexible on choosing the appropriate deductible from SGD25,000 to SGD75,000 depending on the character of your industry risk
- Flexible cover selection
- 24/7/365 Emergency Response Support

Our Cyber Insurance Product

Preferable Risk

- Size of the company
  Turn Over: Less than SGD250 m
  # of PII (Personal Identical Information): Less Than 250,000

- Nature of Business
  Manufacturer
  Healthcare
  Hospitality
  Retail
  Professional Services (e.g. Lawyers/Accountants/Architect/Engineers)
  Financial Institutions (e.g. Investment Managers/Insurance brokers)
  Oil and Gas

Required Information
- Proposal Form
- Web sited or company's brochure
- Larger companies (exceed above criteria)– Supplemental Questionnaire

Our Cyber Insurance Product

NOT Preferable Risks

- Nature of Business
  - Payment Processing
  - Cryptocurrency
  - FINTEC
  - Debt Collector
  - Government
  - Gambling & Casinos
  - Online Gambling & gaming
  - Debt Collector
  - Social Media/Dating Website