Cyber Insurance
Product and market update
BINUS University Graduates Program Students
Premiro brings you to the latest innovation in buying insurance.

Our mission is directed toward a simpler and faster way to procure insurance without the hassle and paper mess that it is commonly associate with.

PT Mitra Ibisnis Terapan (MIT) is a technology-based insurance broker that backed by MIR Insurance Broker, and we know exactly what it takes to unite the insurance complexity and technological simplification.

PT Mitra Ibisnis Terapan is registered and fully licensed as a Digital Insurance Intermediary and supervised under Indonesia Financial Authorities (OJK)
Agenda

Insurance 101

Cyber Insurance Product

What Insurance asked from Client

Current Market Update
Insurance 101

Life insurance was founded in London 1706. Accident insurance was created in 1848 England.

National Insurance (e.g. Pension, Medical) was created in 1880 Germany.

Insurance is constantly developing throughout the years.

As technology advances, new insurance will be developed.
WHAT IS INSURANCE

A contract between an insurer and insured that gives financial protection against insurable loss

Offer and acceptance basis (Contract law)

**Insurable Risks**
- Insurance will be able to insure
- Different Insures have different appetite

**Uninsurable Risks**
- Not enough information
- Unacceptable Risks
  - High Claim Ratio
  - Against the Law
  - Political Risks
- Pandemic Risks
- Natural Disaster Zone
Principles of Insurance

1. **Utmost Good Faith.** Insured need to disclose all relevant facts that will affect the insurance terms and conditions. If any facts are hidden from the insurer, the insurer has the right to void.

2. **Insurable Interest.** The person who purchased the insurance will need to have a pecuniary interest.

3. **Indemnity.** Insurer provide financial compensation to place insured to the original position before the loss.

4. **Contribution / Co-insurance**

5. **Subrogation.** Once the claim has been paid, the right of ownership of the property will be insurer’s. The insured will not be able to make a profit from the damaged property.
Cyber perils are the biggest concern for companies globally in 2022, according to the Allianz Risk Barometer.

The threat of ransomware attacks, data breaches or major IT outages worries companies even more than business and supply chain disruption, natural disasters or the Covid-19 pandemic, all of which have heavily affected firms in the past year.
Allianz Risk Barometer 2022: Top concerns around the world

The graphics show the top three risks in selected countries and whether each risk is considered to be more or less important than 12 months ago or is in the same position.

Australia
1. Business interruption
2. Cyber incidents
3. Climate change
Business interruption and cyber share the top spot with 41% of responses

Brazil
1. Cyber incidents
2. Natural catastrophes
3. Business interruption
Natural catastrophes is the biggest risk riser, moving up from sixth position

Canada
1. Business interruption
2. Cyber incidents
3. Climate change
Climate change moves up to its highest-ever position

China
1. Business interruption
2. Cyber incidents
3. Market developments
Business interruption is the new top risk with 36% of responses

Japan
1. Cyber incidents
2. Natural catastrophes
3. Business interruption
Cyber is the top risk for the second year in a row with 63% of responses

Kenya
1. Business interruption
2. Political risks and violence
3. Pandemic outbreak
Political risks and violence is a new entry in second position

Nigeria
1. Cyber incidents
2. Political risks and violence
3. Macroeconomic developments
Cyber is the top risk for the first time with 46% of responses

Singapore
1. Business interruption
2. Cyber incidents
3. Pandemic outbreak
Pandemic moves up to joint second top risk with 42% responses

What Our Insurance See – Cyber Risk

1. Cyber incidents ranks as a top three peril in most countries surveyed.
2. The main driver is the recent surge in ransomware attacks, which are confirmed as the top cyber threat for the year ahead by survey respondents (57%).
3. Recent attacks have shown worrying trends such as ‘double extortion’ tactics combining the encryption of systems with data breaches; exploiting software vulnerabilities which potentially affect thousands of companies (for example, Log4J, Kaseya).
4. Cyber security also ranks as companies’ major environmental, social and governance (ESG) concern to build resilience and plan for future outages.
5. “Ransomware has become a big business for cyber criminals, who are refining their tactics, lowering the barriers to entry for as little as a $40 subscription and little technological knowledge.
6. The commercialization of cyber crime makes it easier to exploit vulnerabilities on a massive scale. We will see more attacks against technology supply chains and critical infrastructure.

Highlight – Cyber Insurance

- Business interruption loss
- Claims preparation costs
- Direct financial loss
- Extortion loss
- Crisis management costs
- Data restoration costs
- Privacy response costs; or Regulatory penalties and/or Regulatory costs.
- IT forensic investigation costs
What is Cyber Liability Insurance?

Coverage

1. Cyber Liability covers financial losses from data breaches and cyber events including, Legal, IT Forensics, Data Restoration, Breach Notification to customers and Public Relations.
   - First Party - cover Insured out-of-pocket expenses, including incident response from:
     - Cyber Extortion / Ransomware
2. Data Asset Loss & Recovery Expenses
3. Business Interruption
4. Third Party Liability – cover lawsuits from 3rd party due to negligence from:
5. Network Security and Data Privacy
6. Electronic Media
7. Important: Cyber liability is different from Cyber Crime
How to set the LOL of Cyber Insurance?
The Right and appropriate Limit will be one of
The Successful Cyber Insurance Policy adoption

Broker will help the clients to understand current Market and how the Underwriter Requirement for Cyber Insurance

We Need to understand the Business Process to understand the Risk Exposure and map to the right Cyber Insurance Terms

Insurers have significantly raised the bar on the security standards required to purchase cyber insurance. Customer need to Catch Up.

How to set the LOL of Cyber Insurance? The Right and appropriate Limit will be one of The Successful Cyber Insurance Policy adoption
1st Party Coverages

Cyber Extortion. Covers cyber extortion or ransomware from cyber attacks.

Electronic Data Recovery. Cover investigation and restoring costs from cyber attacks or data breach, if possible.

Business Interruption. Cover financial losses (loss of profit) that caused Computer System or Network unable to operate due to cyber events.
3rd Party Coverages

Network & Data Privacy Liability. Cover breach or contamination of personal/corporate data/information in result from unauthorized 3rd party access from and the failure to prevent security breach from virus or Denial of Service (DoS). Also cover defense costs

Electronic Media Liability. Covers lawsuits against the insured from acts of libel, slander, defamation, copyright infringement or invasion of privacy on the Internet.
What is Cyber Crime?

Cyber Crime Insurance covers First Party from monetary/financial losses from:

1. Electronic / Computer Crime from ‘hacking’ losses
2. Ransom demands
3. Unauthorized Calls (extension available)
4. Credit card forgery (extension available)
5. Social Engineering Fraud (extension available)

Cyber crime insurance is hardening; therefore, the capacity is limited, and rate is high.
Cyber Liability vs Crime Comparison

**Cyber Liability Covers**
Cover 1st and 3rd Party from Data Privacy Infringement, Ransom, Business Interruption and Data Losses from Network Security Breaches.

**Cyber Crime Insurance Covers**
Covers 1st party from financial losses from Cyber Hacking, Fraud, Credit Card Forgery and Social Engineering.
Highlight – Claim Process

- Claim Scenario - Examples
- Claim Definition
- Claim Expense Detail
- Understand the exclusions
General Exclusions

- Willfully breach of duty, violations of any Law, Criminal activities, fraudulent, dishonest act or omission.
- Any actual or attempted gain of personal profit, secret profit or advantage by you to which you were not entitled.
- Bodily Injury/ Property Damage
- Assumed Liability
- Insured versus Insured
- Employment Related Wrongful Acts
- Fee
- Internet Access (Internet Service Provider)
<table>
<thead>
<tr>
<th>Insuring Agreement</th>
<th>Claim Scenario</th>
<th>What is covered?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and Information Security Liability</td>
<td>A hacker successfully obtains sensitive personal information from the insured’s computer system. As a result, several donors bring a claim against the insured for allowing access to their personal information.</td>
<td>Damages and Defence Costs</td>
</tr>
<tr>
<td>Communication and Media Liability</td>
<td>A lawsuit is brought against the insured by another non-profit entity alleging that their online content and organizational branding have been plagiarized and their trademarks infringed upon.</td>
<td>Damages and Defence Costs</td>
</tr>
<tr>
<td>Regulatory Defense Expenses</td>
<td>A charity with offices nationwide suffers a major data breach involving thousands of donors. As a result, Attorneys General in multiple states bring regulatory action against the insured.</td>
<td>Regulatory Costs from Data Breach</td>
</tr>
<tr>
<td>Insuring Agreement</td>
<td>Claim Scenario</td>
<td>What is covered?</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Breach Remediation and Notification</td>
<td>A skilled cyber criminal hacks into the insured’s internal processing system. Names, addresses, and credit card information for over 50,000 of the insured’s members are captured out of the system</td>
<td>cost of hiring breach response firm and fixing the breach</td>
</tr>
<tr>
<td>Computer Program and Electronic Data Restoration</td>
<td>A computer virus destroys the insured’s operating system software and data.</td>
<td>Cost for repair and restoration</td>
</tr>
<tr>
<td>Business Interruption</td>
<td>An organization’s server is infected by a severe virus; and as a result, their donation website is not available for an extended period.</td>
<td>Net losses from computer system disruption</td>
</tr>
<tr>
<td>Insuring Agreement</td>
<td>Claim Scenario</td>
<td>What is covered?</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Computer Fraud</td>
<td>An organized crime ring gains unauthorized access to the insured’s accounts payable in their computer system and alter the bank routing information on outgoing payments. The result - $1 million transferred to the crime ring’s account</td>
<td>Direct loss of insured money</td>
</tr>
<tr>
<td>Funds Transfer Fraud</td>
<td>An insured receives an email that appeared to be from its bank but was not. The insured’s employee opened the email, which activated a computer virus called a Trojan horse that reads keystrokes from their computer. The perpetrator used this means to obtain banking and password information and initiate a fraudulent electronic wire transfer from the insured’s bank account.</td>
<td>Funds that were fraudulently transferred</td>
</tr>
<tr>
<td>Insuring Agreement</td>
<td>Claim Scenario</td>
<td>What is covered?</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>E-commerce extortion</td>
<td>The insured receives a series of notes which threaten to hack into its customer database and disclose all the contact information to the general public.</td>
<td>Money paid to extortioner</td>
</tr>
<tr>
<td>Business Interruption</td>
<td>Server unable to operate due to ransomware</td>
<td>Net losses from computer system disruption</td>
</tr>
</tbody>
</table>
## Comprehensive Crime Insurance Market Information
**Banks in Indonesia and other regions (2017-2021)**
*All Figures in US Dollar*

<table>
<thead>
<tr>
<th>Banks</th>
<th>Limit of Liability</th>
<th>Deductible Company Reimbursement - Indonesia territory</th>
<th>Deductible Company Reimbursement - Rest of the world</th>
<th>Premium/annum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset above IDR 50 Trillion</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank A</td>
<td>10,000,000</td>
<td>100,000</td>
<td>100,000</td>
<td>150,000</td>
</tr>
<tr>
<td>Bank B</td>
<td>15,000,000</td>
<td>50,000</td>
<td>50,000</td>
<td>180,000</td>
</tr>
<tr>
<td>Bank C</td>
<td>25,000,000</td>
<td>50,000</td>
<td>50,000</td>
<td>350,000</td>
</tr>
<tr>
<td><strong>Asset between IDR 10 Trillion up to IDR 50 Trillion</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank D</td>
<td>5,000,000</td>
<td>25,000</td>
<td>25,000</td>
<td>90,000</td>
</tr>
<tr>
<td>Bank E</td>
<td>10,000,000</td>
<td>25,000</td>
<td>50,000</td>
<td>145,000</td>
</tr>
<tr>
<td>Bank F</td>
<td>15,000,000</td>
<td>100,000</td>
<td>100,000</td>
<td>165,000</td>
</tr>
<tr>
<td><strong>Asset between IDR 1 Trillion up to IDR 10 Trillion</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank G</td>
<td>2,000,000</td>
<td>50,000</td>
<td>50,000</td>
<td>40,000</td>
</tr>
<tr>
<td>Bank H</td>
<td>8,000,000</td>
<td>50,000</td>
<td>50,000</td>
<td>130,000</td>
</tr>
</tbody>
</table>
Basic Controls
Demonstrating Cyber Preparedness

These control categories are NOT an exhaustive list of all insurer requirements. Multiple factors are considered by each individual insurer when evaluating an organization. However, the consistent message from cyber insurers has been that the controls discussed are the ones they find most important at this time.
Access management

SAMPLE APPLICATION QUESTIONS

• How does the organization manage privileged accounts?
• How many users have persistent privileged accounts for servers and endpoints?
• How many service accounts does the organization have?
• How does the organization evaluate permissions for administrator accounts and service accounts?
• How often are privileges reviewed?

INSURERS’ GENERAL BASELINE REQUIREMENT

• Limit the number of privileged accounts for critical systems and/or processes to one, but no more than two.
• Establish a process to periodically review privileged accounts.
Authentication procedures

Means used to verify the identity of the user attempting to access any information, data, platforms and/or applications. Typically, these will involve a combination of something the user knows (e.g., password), something the user has (e.g., a token/verification code), and/or something the user is (e.g., fingerprint).

SAMPLE APPLICATION QUESTION

Does the organization have multifactor authentication enabled on all user accounts?

INSURERS’ GENERAL BASELINE REQUIREMENT

Enable multifactor authentication for remote access, administrator accounts and email, and have at least two authentication measures in place, e.g., password and token.

Multifactor authentication should be enabled for organizations using cloud-based solutions to house sensitive information.
Backup policies

Measures that duplicate the organization’s data and systems so that they can recreate the data and systems if there is an incident, instead of starting from the beginning.

SAMPLE APPLICATION QUESTION

What are the organization’s standards for backups?

INSURERS’ GENERAL BASELINE REQUIREMENT

Backup critical information at least weekly, and segment and encrypt those backups.
Blocking & filtering solutions

Mechanisms used to limit the potential for compromises as a result of malicious emails, links, websites, and other unauthorized attempts to gain access to the systems and network.

**Perimeter blocking and filtering solutions**

Tools that scan, filter and block malicious network activity, and can include an Intrusion Prevention System (IPS) deployed upon finding malicious activity and/or an Intrusion Detection Solution (IDS) which only detects and sends an alert to administrators in the event of suspicious activity.

**SAMPLE APPLICATION QUESTION**

Does the organization have an intrusion prevention or detection solution in place?

**INSURERS’ GENERAL BASELINE REQUIREMENT**

Not mandatory at this time, but favorable consideration provided to those organizations using intrusion prevention or detection tools.
Blocking & filtering solutions

Email blocking and filtering solutions

Tools that block spam, phishing and viruses from reaching and/or leaving a user’s email account and can include the following protocols: Sender policy framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC) —

SAMPLE APPLICATION QUESTIONS

Does the organization filter/scan incoming emails for malicious attachments and/or links?

Does the organization have the ability to automatically quarantine, destroy and evaluate attachments?

INSURERS' GENERAL BASELINE REQUIREMENT

Use tools that block and filter emails to limit the potential for compromises as a result of a malicious email, link and/or attachment.
Blocking & filtering solutions

Web blocking and filtering solutions
Systems that block access to malicious, dangerous or inappropriate content from websites.

SAMPLE APPLICATION QUESTION
Does the organization route all outbound web traffic through a web proxy which monitors for and blocks potentially malicious content?

INSURERS’ GENERAL BASELINE REQUIREMENT
Utilize a web proxy to limit the potential risks from everyday internet usage.
Cybersecurity awareness & training

Policies and procedures to train an organization’s workforce to ensure good cyber hygiene habits, increase awareness of risk and promote an organizational culture of mindfulness around cybersecurity and privacy rights. These policies can include simulated phishing attacks, training seminars and privacy compliance exercises.

SAMPLE APPLICATION QUESTION

Does the organization simulate phishing attacks to test its workforce’s cybersecurity awareness?

Does the organization conduct mandatory information security and privacy training of employees and contractors?

INSURERS’ GENERAL BASELINE REQUIREMENT

Test workforces’ susceptibility to phishing attacks annually and implement annual training on cybersecurity and privacy protection compliance.
End-of-life support software

No longer receives patches/updates from the vendor and is extremely vulnerable to attacks. Without patching, threat actors have the ability to try to exploit vulnerabilities for a much longer period of time, often undetected.

SAMPLE APPLICATION QUESTIONS

If organization has any end-of-life or end-of-support software, is it segregated from the rest of the network?

Does the organization have a process to decommission unused systems?

INSURERS’ GENERAL BASELINE REQUIREMENT

Identify, segment and establish a process for sunsetting and removal from inventory.
Endpoint detection & response tools (EDR)

Mechanisms used to secure end user devices, such as laptops and mobile phones. EDR tools are behavior focused, i.e., “should this application be doing this activity with this user at this time with these files”? EDR is not the same as antivirus software (e.g., Webroot, ESET, Bitdefender, McAfee) which looks for malicious files as compared to a known “clean” version of the same file.

SAMPLE APPLICATION QUESTION

Does the organization use an endpoint protection and response product across its workstations?

INSURERS’ GENERAL BASELINE REQUIREMENT

Use detection tools to examine files as they enter the network and employ a product to respond to any malicious activity or threat source.
Incident response and business continuity plans

Written policies that identify the key steps that will need to occur to: Respond to the incident; and continue business operations in the event of an incident. These documents serve as the roadmap for responding to the incident and continuing business operations when an incident occurs. These plans should be printed and stored in multiple locations, so that they are accessible during an incident.

SAMPLE APPLICATION QUESTIONS

Does the organization have a written incident response plan to address cyberattacks?

Does the organization have a written business continuity plan to address cyberattacks?

INSURERS’ GENERAL BASELINE REQUIREMENT

Written plans that are tested at least once a year to assess the ability to respond and restore critical systems, information, and operations.
Network and infrastructure segmentation

An architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. While improving performance, more importantly, segmentation provides additional security, i.e., if a network is segmented a threat actor may be able to infiltrate one segment, the chances of infiltrating others and compromising the entire network are diminished.

SAMPLE APPLICATION QUESTIONS

Does the organization segment its network based on certain criteria, such as: classification or level of information stored, geography and business function?

Does the organization segregate critical networks from internet facing or other less critical networks?

Does the organization segregate operational technology from information technology networks?

INSURERS’ GENERAL BASELINE REQUIREMENT

Segment at multiple levels, including classes of information, business function and geography — specific requirements will vary by insurer, class of business and organization size.
Patches/updates

Measures to protect software applications when a security flaw is discovered in them. The software developer typically creates a replacement program and/or file, i.e., “patch” to eliminate flaws discovered in earlier versions.

SAMPLE APPLICATION QUESTION

What is the organization’s timeframe to implement critical patches?

INSURERS’ GENERAL BASELINE REQUIREMENT

Critical patches should be implemented within 24 to 72 hours with less critical patches being implemented within two to seven days.
Security monitoring

Mechanisms employed by the organization to actively monitor security and can include a Security Incident Event Management (SIEM) system which collects and analyzes aggregated log data from the organization's network and platforms and a Security Operations Center (SOC) which consists of people, processes, and technology designed to address logged security events.

SAMPLE APPLICATION QUESTIONS

Does the organization utilize a SIEM monitored 24/7 by a SOC?

Does the organization have staff dedicated to monitoring security operations?

Is that staff available 24/7?

Does the organization outsource its security operations to a third party?

Does the organization monitor active directory or have an identity and access management platform to detect unusual activity or abnormal behavior?
Asia composite insurance pricing change — by major coverage line

Financial and professional lines pricing rose 17%, the same as in the third quarter.

Insurers focused on risk selection, with D&O accounting for a significant portion of pricing increases.

Cyber remained the most challenging coverage area, driven by ransomware claims, with considerable pressure on pricing and deductibles, a reduction in capacity, and narrowing of key coverages.
Financial and professional lines pricing rose 17%, the same as in the third quarter. It was the eleventh consecutive quarter of increase (see Figure 4).

Insurers focused on risk selection, with directors and officers (D&O) liability coverage for large organizations driving a significant portion of pricing increases.

Asia continued to be a fragmented marketplace, with pricing movements not aligned between clients and countries.

Cyber risk, driven by ransomware losses, remained the most challenging coverage area, with increased pressure on pricing, deductibles, and capacity, and a narrowing of coverage.
Conclusion

1. Digitalization and cyber-attacks are increasing relentlessly - among companies.

2. Supply and demand for cyber insurance have increased slightly, but most respondents are still not adequately protected or even prepared.

3. The potential for cyber insurers is high, but resilience and readiness are a prerequisite for tapping into this potential.

4. It is the duty of the insurance industry to explain the importance of resiliency measures on risk exposure to their clients and customers – and this would include discussing influencing factors such as premiums, prices, coverages, limits, terms and conditions, and access to insurance.
Conclusion

5. Cyber insurance, can leverage to reshape cyber risk assessment and better explain the modelling of cyber risks to its insured. Overall, better data analysis can identify causal factors of a particular claim and identify the best means of risk mitigation.

6. As a basic tenet, insureds should not be rewarded for having basic controls in place – this should be a mandate for risk eligibility. But the minimum acceptable thresholds should be continuously evolved to mirror the greatest threats to an insured at any given time.

7. Finally, in this context, it is worth underlining that collecting data is just one half of the equation – the data must also be useful in terms of analysis and the insurance industry must have the capabilities to analyze and share it in a meaningful way.