About MSIG Indonesia

PT Asuransi MSIG Indonesia, part of the MS&AD Insurance Group, is a general insurance company in Indonesia that has been operating since 1975 and continues to grow. With years of experience, we bring our deeply rooted values. We look beyond the things insured and see the heart in everything.

Our mission is to contribute to the development of a vibrant society and help secure a sound future of the planet, by enabling safety and peace of mind through the global insurance and financial services business.

For further information about the product, please scan the following QR code:

HEAD OFFICE :

PT Asuransi MSIG Indonesia

Summitmas II Building, 15th Floor
Jl. Jenderal Sudirman Kav. 61 - 62
Jakarta 12190, Indonesia

Phone : (021) 252 3110 (Hunting)
Fax : (021) 252 6761 (General)
Email : msig@id.msig-asia.com
URL : www.msig.co.id

msigid | msig_id | @msig_id | MSIG Indonesia

COMPLAINT SERVICE CONTACT :
Phone : (021) 252 3110 (Hunting)
Email : customer@id.msig-asia.com

BRANCH & REPRESENTATIVE OFFICE :

Bandung | Phone (022) 3000 0851, 3000 0852 - idn_bandung@id.msig-asia.com
Batam | Phone (0770) 611 550, 611 161 - idn_batam@id.msig-asia.com
Denpasar | Phone (0361) 471 7227, 471 7228 - idn_denpasar@id.msig-asia.com
Medan | Phone (061) 452 8783, 452 8795 - idn_medan@id.msig-asia.com
Palembang | Phone (0711) 563 0711, 563 0712 - idn_palembang@id.msig-asia.com
Semarang | Phone (024) 841 7010, 841 7013 - idn_semarang@id.msig-asia.com
Surabaya | Phone (031) 531 8876, 531 8496 - idn_surabaya@id.msig-asia.com

IPB-V65-E2-2024-10

PT Asuransi MSIG Indonesia is licensed and supervised by Financial Services Authority (OJK)

MSIG

This brochure only contains general information about MSIG Cyber Insurance and does not define an insurance contract/agreement. Details of the conditions of coverage and exclusions are stated in the Policy. The Insured must read and understand the Policy.

MSIG CYBER INSURANCE

Cyber Safeguard for Your Business Peace of Mind

MSIG Insurance that sees the heart in everything

A Member of MS&AD INSURANCE GROUP

PAHAMI & MILIKI SURANSI

MSIG Cyber Insurance

Cyber Safeguard for Your Business Peace of Mind

Indemnify you or pay on your behalf in excess of the applicable retention of:

1. Investigation cost
2. Response cost
3. Restoration cost
4. Interruption
5. Liability
6. Extortion loss
7. Regulatory

Arising due to breach of confidentiality, breach or privacy or security breach

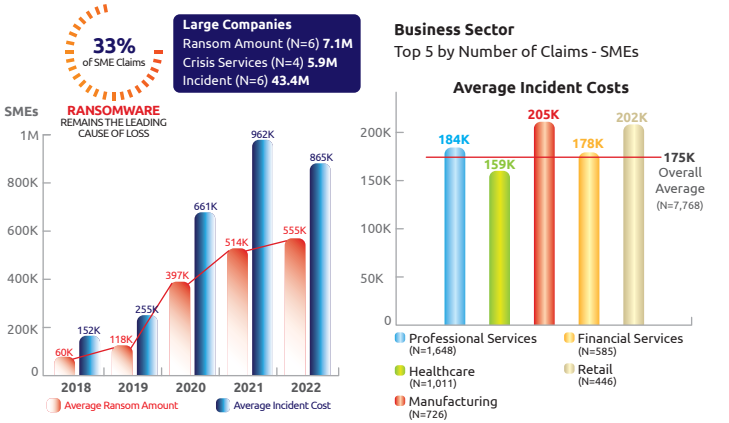
We will provide the cover described in the Policy, subject to its terms and conditions, for the Policy period.

Why Do We Need Cyber Insurance?

Cybersecurity trends in Indonesia have been evolving rapidly as the country's digital landscape grows.

- **Increase in Cyber Attacks:** Indonesia has seen a rise in cyberattacks, including ransomware, phishing, and data breaches. As more businesses and individuals go online, the opportunities for cybercriminals grow.
- **Ransomware Threats:** Ransomware attacks are becoming more frequent and sophisticated. These attacks often target critical infrastructure and large organizations, demanding hefty ransoms for data recovery.
- **Phishing and Social Engineering:** Phishing attacks, including spear-phishing, have been prominent. Cybercriminals use these tactics to trick individuals and organizations into revealing sensitive information.
- **Data Privacy Concerns:** With new regulations like the Personal Data Protection Law (PDP Law) enacted in 2022, there is increased emphasis on data protection. However, there are still challenges in implementing and enforcing these regulations effectively.
- **Public Awareness and Training:** There is a growing focus on increasing cybersecurity awareness and training among individuals and organizations to better defend against cyber threats.
- **Emerging Threats:** The rise of Internet of Things (IoT) devices and cloud computing introduces new vulnerabilities. Cybercriminals are increasingly targeting these areas to exploit weak security measures.
- **Overall Cyber Incident Cost:** If it happens to you, a breach or cyber incident could wind up costing you to the tune of hundreds of thousands of dollars.

Average Costs from Ransomware



Source: Net Diligence

Below are some actual cases of cyber incident in Indonesia:

1. In 2023, one of the largest Islamic banks in the country, experienced a severe cyberattack. This attack involved ransomware that targeted the bank's digital infrastructure, encrypting critical data and disrupting its services. The ransomware attack caused significant operational disruption, affecting banking services and customer access to their accounts. It also raised concerns about the security of financial institutions in Indonesia. The attack led to a temporary halt in some services and prompted the bank to work closely with cybersecurity experts to resolve the issue and strengthen its security posture. The incident highlighted the need for improved cybersecurity practices within financial institutions.

2. In 2024, there was a significant data breach involving the National Cyber and Crypto Agency (BSSN). This breach exposed sensitive information related to the agency's cybersecurity operations and internal communications. The breach raised serious concerns about the security of Indonesia's cybersecurity infrastructure and the agency responsible for national cyber defense. It highlighted the potential risks of insider threats and the need for more stringent security practices. The BSSN, in collaboration with other government bodies and cybersecurity experts, took immediate actions to address the breach, secure affected systems, and enhance internal security measures. The incident also prompted a review of national cybersecurity strategies.

Coverage

1. **IT Forensic Investigation Costs**
   Covers the cost of external IT security experts. Including costs of legal advisors to appoint, oversee and guide external IT security experts.
2. **Privacy Response Costs**
   Covers costs that are incurred as a result of a Breach of Privacy.
3. **Data Restoration Costs**
   Covers costs on the Insured's behalf where data has been corrupted, erased, encrypted, damaged, or destroyed. Including costs for recovery, restoration, input, configuration, or replacement.
4. **Business Interruption Loss**
   Covers costs when an Insured is unable to use data assets for business activities.
5. **Liability**
   Covers legally obliged payment on the Insured's behalf of third party's data assets' damages due to Breach of Confidentiality, Breach of Privacy or Security Breach.
6. **Extortion Loss**
   Covers loss due to threats resulting disclosure of confidential information, corrupted data assets, and impairment of computer system availability.
7. **Regulatory Penalties/Costs**
   Covers regulatory penalties and related regulatory costs resulting from Breach of Privacy.

PREMIUM RANGE FOR SME BUSINESS

Annual Gross Revenue (USD)	Limit of Indemnity (USD)				
	250,000	500,000	1,000,000	1,500,000	2,000,000
500K - 2 mio	1,300 - 1,600	1,650 - 1,900			
2 mio - 5 mio	1,600 - 1,900	1,900 - 2,300			
5 mio - 10 mio	1,900 - 2,500	2,300 - 3,100	3,100 - 3,900	4,700 - 4,900	5,900 - 6,200
10 mio - 15 mio	2,500 - 3,500	3,100 - 4,400	3,900 - 5,500	4,900 - 6,800	6,200 - 8,300
15 mio - 25 mio	3,500 - 5,700	4,400 - 7,000	5,500 - 8,700	6,800 - 11,200	8,300 - 13,600
25 mio - 35 mio	5,700 - 8,000	7,000 - 9,800	8,700 - 12,300	11,200 - 15,200	13,600 - 18,500
35 mio - 50 mio	8,000 - 10,900	9,800 - 13,150	12,300 - 16,400	15,200 - 21,000	18,500 - 25,700

Note:

1) Above table are range premium based on the annual gross revenue and limit of indemnity for standard coverage only.
2) The final premium will be depend on the actual annual gross revenue amount of the prospect customer.
3) Final Premium can be outside of the premium range in above depends on UW consideration after analyze information in the Proposal form.
4) Generally, the range premium above can be applied if the criteria on the proposal form are fulfilled (answer as "Yes" for query on the Section 2 Question A and Section 3 Question A-K).

Extended Coverage (Optional)

1. **Business Interruption and Restoration Costs as a Result of an Operational Error**
   Covers damages of data assets and computer system caused by employee's unintentional error.
2. **Media Liability**
   Covers damages and claim costs arising out of a claim for content violation.
3. **Personal Information Violation**
   Covers damages and claim costs arising out of a "personal information violation".
4. **Payment Card Industry (PCI)**
   Covers payment as a result of a payment card breach. (This section is only relevant to Insured that process or store payment card information).
5. **Reputational Interruption Loss**
   This will indemnify the Insured for business interruption loss directly and solely attributable to impairment of brand/reputation.
6. **Cyber Crime**
   Covers direct financial loss sustained as a direct result of having transferred funds due to:
   - Reliance on a fraudulent, dishonest or criminal input of verified instructions to your computer system or your data assets.
   - Access to your computer system or your data assets was gained as a result of asecurity breach.

Kindly be noted that additional premium will be apply for above additional insuring agreement.

Product Benefit

- Flexible product that can be scoped to fit coverage needs and budget.
- 24/7 incident helpline. Expert vendors will provide the expertise at each point of incident process; IT Forensic Investigation/Public Relations/Call Centre/ID Protection etc.

Exclusion

1. Bodily Injury
2. Contractual Liability
3. Dishonest Acts
4. Illegal Programs
5. Infrastructure
6. Insolvency of Insured or a Third Party
7. Physical Event
8. Prior Act
9. Property Damage

Others as per Policy Wording

MSIG INCIDENT RESPONSE PROCESS

The MSIG Cyber panel Experts and legal advisors are working on behalf of MSIG's insured as part of the 24/7 MSIG Cyber Helpline

1. ***Policyholder calls Incident Response Line***
2. ***Response Manager captures key information***
3. ***Response contacts relevant jurisdiction experts***
4. ***Conflict Checks check- escalation if conflict issue arises***
5. ***Contact Policyholder conducts triage (within 2 hours)***
6. ***Response Manager scopes call/considers appointment of vendors***
7. ***Response Manager produces 24/48 hour report***
8. ***Manages incident with agreed reporting matrix/ template report form to be completed***
9. ***Resolve incident***
10. ***Review meeting with Policyholder – lesson learnt***