

MALAYSIAN RE FORESIGHTS

ISSUE 7 | April 2025

PUBLISHED BY



RECOGNISED REPUTABLE RELIABLE

Fitch Ratings 'A' (Strong) with a Stable Outlook.

A.M. Best 'A-' (Excellent) with a Stable Outlook.



CYBERSECURITY RISK IN MALAYSIA

Cybersecurity risk has become a priority concern for businesses as they move increasingly swiftly towards digital platforms. This potentially results in increased risks of cyberattacks across various industries, regardless of size.

The growing reliance on technology and the increasing value of data collected have created new corporate risks and hazards. Cyberattacks have become a major threat to businesses. This can potentially cause catastrophic financial and reputational harm. The key cybersecurity risks are:

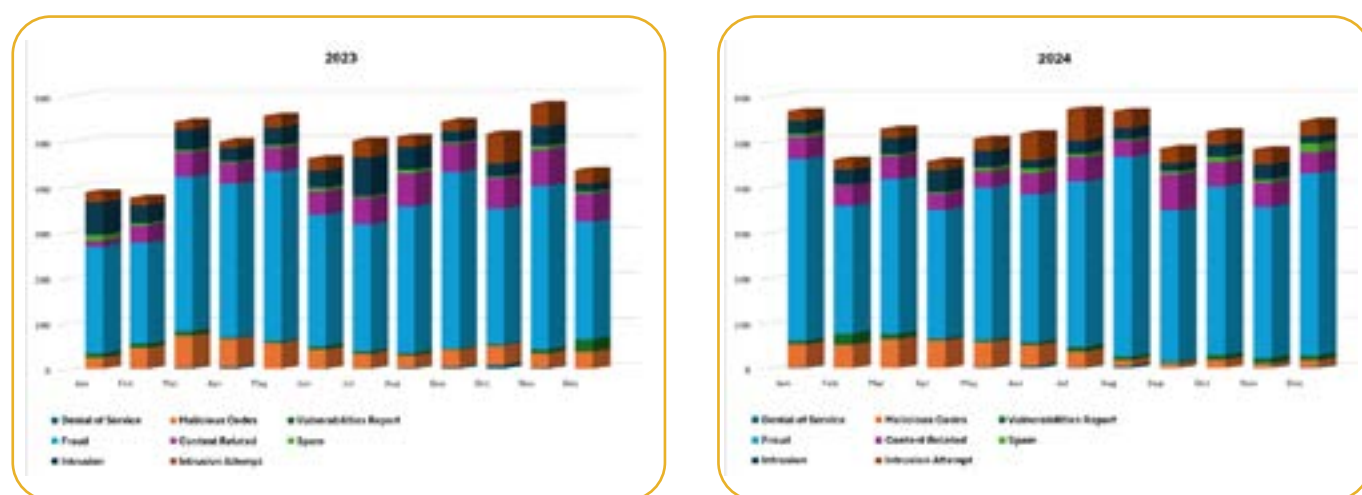
1. Ransomware attacks—Cybercriminals target businesses and government agencies, encrypting data and demanding payment to restore access. The ransomware costs, including ransom payments, data recovery, and operational downtime, can severely damage businesses.
2. Data breaches are a growing concern, and sensitive customer information from industries like finance, healthcare, and e-commerce is a valuable target for cybercriminals. Breaches can result in regulatory fines, reputational damage and legal liabilities.
3. Phishing and social engineering are attacks in which attackers impersonate legitimate entities to trick individuals into revealing sensitive information.
4. Insider threats occur when employees or contractors misuse their access to corporate systems to steal data, commit fraud or cause damage.
5. Internet of Things (IoT) vulnerabilities – The rise of IoT devices such as smart home systems, industrial sensors and healthcare devices poses a new security risk. These devices often have weak security measures, making them vulnerable entry points for cybercriminals. When IoT devices are compromised, they can have a cascading effect on the entire system. Here is how:
 - (i) Network infiltration: once an attacker gains access through an IoT device, they can infiltrate the broader network. This can lead to unauthorized access to other devices and systems connected to the same network.
 - (ii) Data exfiltration: compromised IoT devices can be used to steal sensitive data. This includes personal information, corporate secrets, and other sensitive and critical data which can then be exfiltrated to the attacker.
 - (iii) Service disruption: attacks on IoT devices can disrupt services provided. For example, in smart homes, compromised devices can lead to security breaches, while in industrial settings, production processes can be halted.
 - (iv) Propagation of malware: IoT devices can be used to spread malware throughout the network. This can lead to widespread infections, affecting multiple devices and systems.
 - (v) Unauthorized control: attackers can gain control over IoT devices, leading to unauthorized operations. For instance, in healthcare, it could mean altering medical device settings.

Current Cybersecurity Risks Trends and Threats in Malaysia

Like many other countries, Malaysia's cybersecurity landscape is continuously evolving. Threats have grown more sophisticated, with phishing attacks, data breaches and ransomware being the most prevalent.

Based on the latest Kaspersky Security Networks report, Malaysia has risen to 30th place globally for web threats. In 2024, Kaspersky detected and blocked 27.9 million web threats in Malaysia, marking a 4% increase from the previous year (Source: Bernama, January 2025). In 2023, Kaspersky's systems blocked 26.85 million "Internet-borne" attacks in Malaysia, averaging 74,000 daily attacks. Additionally, 22 million "local infection" threats were blocked, equating to 60,000 daily attacks (Source: New Straits Times, February 2024). This data highlights the growing sophistication of cyber threats and emphasizes the urgent need for stronger cybersecurity measures to protect individuals and businesses.

According to Cybersecurity Malaysia, Malaysian Internet users increased to 33.59 million at the start of 2024. As of January 2024, Malaysia's estimated number of social media users is 28.68 million, equating to 83.1% of the total population. Cybersecurity Malaysia reported 6,209 cyber threat cases for the whole year 2024 compared to the previous corresponding period in 2023, the cases reported were only 5,917 cyber threat cases which indicated a 5% increase.



Types of cyberattacks and their incidence in 2023 & 2024 (Source: Cybersecurity Malaysia)

Human error is the major concern as attackers increasingly target this weakest link through fraud attempts. 4,219 fraud cases were reported for 2024, contributing to 67.9 % of the cyber threat cases reported in 2024. Compared to 2023, 3,705 fraud cases were reported, representing an increase of 13.9%.

These incident reported numbers are likely underestimated due to underreporting of cyber threat incidents. This can be attributed to several factors such as (1) lack of awareness, many individuals and organizations may not recognize certain activities as cyber incidents or may not be aware of the importance of reporting them. (2) Fear of reputational damage: companies might avoid reporting incidents to protect their reputation and avoid losing customer trust. (3) Legal and regulatory concerns: some organizations may fear legal repercussions or regulatory scrutiny if they report the incidents. (4) resource constraints: smaller organizations might lack the resources or expertise to detect and report cyber incidents. (5) perceived ineffectiveness: There may be a perception that reporting incidents will not lead to effective action or resolution. Addressing these issues requires increased awareness, better support systems, and stronger incentives for reporting cyber incidents.

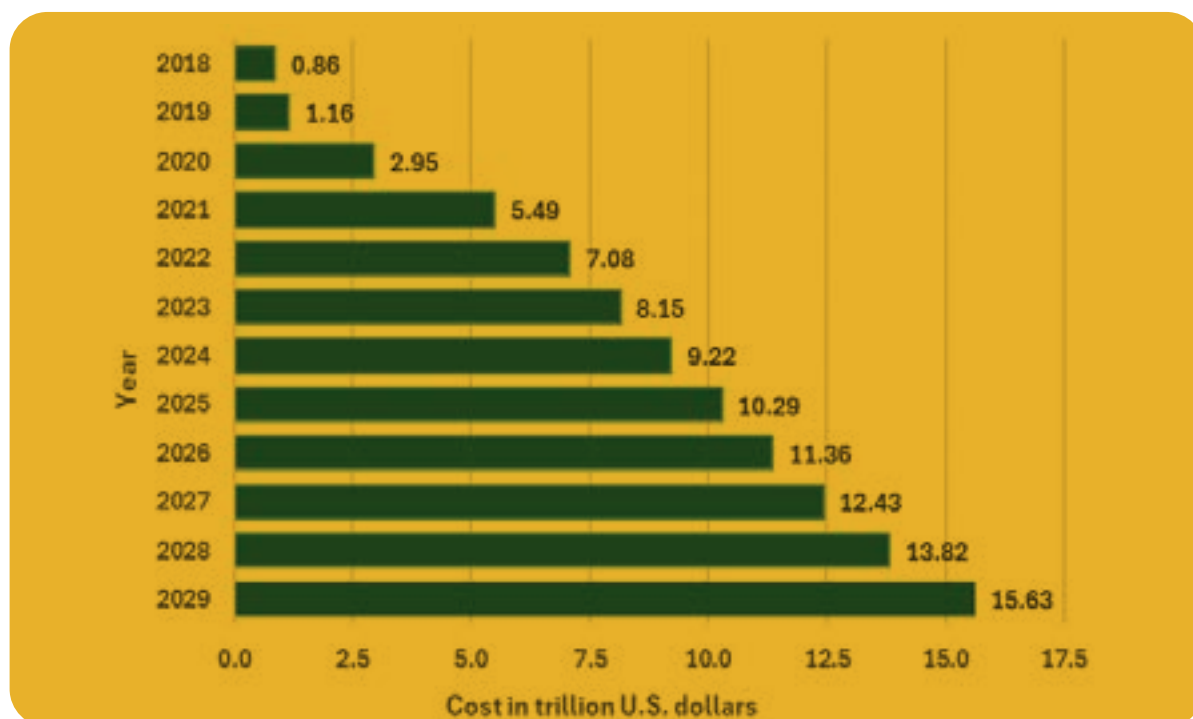
According to the Ensign Info Security Cyber Threat Landscape 2024 report, the top five industry groups observed to be attacked in Malaysia include (1) Manufacturing, (2) Government, (3) Technology, Media and Telecommunications (TMT), (4) Professional Services and (5) Retail. While financial institutions have historically been the primary targets, cyberattacks have shifted to the manufacturing sector. This sector holds a large amount of valuable data and is vital to economic stability and recovery, and the disruption can lead to severe operational and safety issues. Telecommunications and other essential services also attract cyberattacks due to their central role in economic activities.

Nevertheless, PwC highlighted that financial services in Malaysia remain prime targets for cyber attackers due to their high value and the adoption of new technologies. Innovations such as cloud computing and artificial intelligence, along with third-party integrations, expand the “attack surface,” creating more opportunities for cyber threats and increasing organizational vulnerability (*Source: The Edge Malaysia, June 2024*).

Cost of Cyber Attacks

The loss due to cyber threats has become a pressing issue as cyberattacks continue to rise, impacting various sectors of the economy. The financial impact is significant and affects not only individual businesses but the overall economy. However, quantifying the cost of cyber threats is complex and challenging. According to The World Bank, from 2019 to 2023, approximately USD 5.2 trillion globally was at risk from cyber-attacks with 10.5 million records lost or stolen monthly or 438,000 hourly. A single large-scale attack can trigger USD 53 billion in economic losses.

According to Statista, the global indicator ‘estimated cost of cybercrime’ in the cybersecurity market was forecasted to continuously increase between 2024 and 2029 by USD 6.4 trillion, an increase of about 69.4%. The indicator is estimated to reach USD 15.63 trillion in 2029. Notably, the indicator “Estimated Cost of Cybercrime” of the cyber security market has continuously increased over the past years.



Estimated Cost of Cybercrime Worldwide
(Source: <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>)

In a recent case, in July 2024, an automatic update of CrowdStrike’s Falcon sensor software crashed over 8.5 million Microsoft Windows machines globally. Kovrr estimated that this IT outage could cost the UK economy between £1.7 and £2.3 billion. However, global insured losses are projected to be in the mid-to-high single-digit billion USD range and are not expected to significantly impact the re/insurance market. (Source: www.reinsurancene.ws). On the other hand, Parametrix, a company specializing in cloud outage analytics and insurance solutions, estimates that 125 U.S. Fortune 500 firms, excluding Microsoft, will incur approximately USD 5.4 billion in losses due to outages and disruptions. They also project insurance payouts ranging from USD 540 million to USD 1.08 billion (Sources: www.hipaajournal.com, *The Star*, July 2024).

In Malaysia’s context, the IBM 2024 Cost of a Data Breach Report highlighted a growing threat from data breaches across the ASEAN region, including Malaysia. The average cost of a data breach in 2024 rose to USD 3.23 million, marking a 6% increase from USD 3.05 million in 2023. Critical infrastructure sectors were particularly affected, with financial services experiencing the highest breach costs at USD 5.57 million (Source: *New Strait Times*, September 2024).

Cybercrimes in Malaysia have also shown an upward trend. According to police statistics, the number of cybercrimes reported in 2019 was 11,875 cases, with RM498 million in terms of losses. In 2023, the number of cases increased to 14,229, with total losses of RM413 million. In the first quarter of 2024, the number of cases reported was 4,327 and the losses involved were RM77 million (*Source: <https://www.komunikasi.gov.my/en/public/news>, July 2024*).

Cyber Insurance Market Outlook

Cyber insurance can act as a financial cushion in covering the expenses associated with responding to a cyber incident, including forensic investigations, legal fees, notification costs, and crisis management. It also offers compensation for business interruptions, data restoration, and third-party liability claims.

Cyber insurance, like any other type of insurance, provides businesses with compensation if their cybersecurity is compromised. However, the cost of purchasing cyber insurance has risen. This increase is largely due to the growing number of cyber threats. Insurers, in response, have become more cautious and stringent in underwriting policies to mitigate their risks. (*Source: The Edge Malaysia, February 2024*).

Based on the Global Malaysia Cyber Insurance Market Report (Forecast to 2031) by Verified Market Research, the drivers of significant growth in cyber insurance in Malaysia are:

1. The increasing number of cyberattacks: the rise in frequency and sophistication of cyber threats compels businesses to seek insurance coverage.
2. regulatory requirements: governments are enforcing stricter regulations on data protection and driving demand for cyber insurance.
3. growing awareness among businesses: organizations are becoming more aware of potential risks, leading to a proactive approach to securing cyber insurance.

However, there are some restraints highlighted.

1. Limited understanding of cyber insurance products: Many businesses lack awareness of available coverage options and benefits.
2. High premiums for comprehensive coverage: Cost concerns can deter organizations from purchasing adequate policies.
3. Challenges in quantifying risk: The difficulty in assessing potential cyber risks can hinder the adoption of insurance products.

Globally, according to S&P Global, cyber insurance is still the fastest-growing subsector of the insurance market. Global cyber insurance premiums reached about USD 12 billion in 2022 and are likely to increase by an average of 25%–30% per year to about USD 23 billion by 2025. Cyber insurance relies mostly on reinsurance protection, and reinsurers remain critical to the sustainable growth of the market. Cyber insurers use a significant amount of reinsurance. Primary insurers ceded about 50%–65% of cyber insurance premiums to reinsurers in 2023. The reinsurance market and, eventually, the retrocession market will therefore be extremely important in providing capital and capacity to support the growth of the cyber insurance market.

Cyber Claim Management

Cyber claims can vary significantly in nature and complexity. Some common types of cyber claims are:

1. **Data Breach Claims:** These occur when sensitive, protected or confidential data is accessed or disclosed in an unauthorized manner. Data breaches can lead to significant financial losses, legal repercussions, and damage to an organization's reputation.
2. **Business Interruption Claims:** cyberattacks like ransomware can disrupt the normal operation of a business, leading to a significant loss of income. Business interruption claims in the cyber context involve assessing the financial impact of such interruptions.
3. **Cyber Extortion Claims:** this involves threats to release sensitive information or disrupt business operations unless a ransom is paid. These claims require claim professionals to navigate complex legal and ethical considerations.
4. **Identity Theft Claims:** These arise when an individual's personal information is stolen and used for fraudulent purposes. Claim professionals dealing with these types of claims need to assess the financial and emotional impact on the victims.

Managing cyber insurance claims comes with several unique challenges for the claim's professionals:

1. **Complex Technical Aspects:** cyber claims often involve sophisticated technical details that require a deep understanding of IT systems, cybersecurity protocols and digital forensics.

2. **Intangible Losses:** Unlike traditional claims, cyber claims often involve intangible losses such as data breaches, reputational damage and business interruption. Quantifying these losses and determining coverage can be challenging due to:
 - (i) **Ambiguity in Policy Terms:** cyber insurance policies often lack standardized definitions for key terms such as “data breach” or “cyberterrorism” leading to confusion about what is covered.
 - (ii) **Complex coverage Limits and Exclusion.** Policies may have complex coverage limits and exclusions that are not always clear to policyholders. This complexity can make it difficult to understand the extent of coverage, especially in high-risk sectors like healthcare and education.
3. **Proving the Cause and Extent of Damage:** establishing the cause and extent of damage in cyber incidents can be difficult, especially when dealing with sophisticated cyberattacks. This can complicate the process of determining whether a particular incident is covered under the policy.
4. **Evolving Cyber Threats:** The nature of cyber risks is constantly changing with new threats like ransomware, phishing and social engineering fraud emerging regularly. This requires claim professionals to continuously update their knowledge and skills.
5. **Regulatory and Legal Complexities:** cyber incidents are subject to various data protection and privacy laws, varying significantly by region and industry. Navigating these regulations adds another layer of complexity to managing claims.
6. **Documentation and Compliance:** Ensuring all expenses are documented and complying with policy requirements and deadlines can be a meticulous and time-consuming process. This is crucial for proving the claim falls within the coverage scope.

These challenges highlight the need for specialized skills and knowledge in cyber claims management to handle the complexities involved effectively. They also focus on the need for ongoing education and updates to policy terms to keep pace with the rapidly changing cyber landscape.

Collective Efforts

Based on the Global Cybersecurity Index (GCI) 2024, Malaysia is classified as Tier 1 – Role Modelling. This tier includes countries that have achieved an overall GCI score of at least 95/100, showcasing a robust commitment to cybersecurity through coordinated and government-driven actions.

The cyber threats in Malaysia are complex, multi-faceted and evolve at a pace that demands collective action. Public and private partnerships are an important synergy to address cybersecurity concerns.

The government's commitment to cybersecurity can be seen in the adoption of several standards and frameworks such as the National Cyber Security Policy, the Malaysian Common Criteria Evaluation and Certification Scheme, and the Malaysia Trustmark for Private Sector.

In safeguarding Malaysia's cybersecurity infrastructure, the Cyber Security Act 2024 was officially gazetted by the Attorney General's Chambers on 26th June 2024. The Act aims to improve and protect the cybersecurity environment in Malaysia. This legislation is a major milestone in strengthening Malaysia's cyber defences and enhancing resilience against emerging threats.

However, these standards and frameworks are not mandatory for all sectors. Some businesses lack awareness and compliance; hence, some government intervention or policies are required to protect businesses and public safety.

Among the measures that can be implemented are providing incentives or subsidies for companies to adopt cybersecurity measures, encouraging them to obtain cyber insurance, and establishing or enforcing mandatory/voluntary cybersecurity standards for certain industries. Other than that, creating cyber security awareness and education programs for the public and private sectors; facilitating or coordinating cybersecurity information sharing and collaboration among stakeholders.

As a leading national reinsurer, Malaysian Reinsurance Berhad started to provide cyber reinsurance support for the domestic market, especially Personal Cyber and SME Cyber. Malaysian Re offers both Conventional Reinsurance and Retakaful covers, ensuring robust protection for all.

Way Forward

The cyber risk landscape is dynamic, continually evolving with emerging technologies, growing attack vectors and developing regulatory landscapes. As organizations continue to face increasingly sophisticated and persistent cyberattacks, cyber insurance plays a critical role in minimizing potential financial losses and lessening the impact of cyberattacks on organizations.

However, cyber insurers/reinsurers face the challenges of effectively assessing and quantifying cyber risks, which are often complex and rapidly changing. Moreover, the interconnected nature of the digital business world poses systemic risks that could affect several insurance/reinsurance entities at the same time. To keep up with this evolving risk landscape, cyber insurers/reinsurers must continuously adapt their underwriting practices, policy terms and pricing structures.

Cyber insurance can serve as a financial cushion, but it is crucial and imperative for businesses to proactively invest in comprehensive cybersecurity strategies, such as robust security controls and employee training.

*Prepared By:
Nor Afizah Md Zuki*



OPTIMIZING MARINE MACHINERY MAINTENANCE AND LOSS PREVENTION: MINIMIZING CLAIMS AND ENHANCING INSURANCE TERMS

Maintaining reliable marine machinery is crucial as the global economy increasingly relies on marine commerce. The marine industry is the fundamental pillar of global commerce, since more than 80% of the world's goods by volume are transported by sea (Unit, 2022). The role of insurance in maritime operations extends beyond merely covering losses; it is fundamental to promoting safety and reliability within the industry. While insurers are responsible for evaluating risks, establishing premiums, and providing financial protection, they also have a vested interest in reducing the frequency and severity of claims. By prioritizing preventive measures, such as the maintenance and reliability of marine machinery, insurers can significantly reduce the likelihood of costly incidents. This proactive approach ensures the marine industry's long-term sustainability while also safeguarding their financial bottom line.

The Importance of Marine Machinery Maintenance

Consistent and meticulous maintenance upholds vessels' fitness for sailing, functionality, and safety for the crew. This process involves a range of activities, including regular inspections, planned maintenance, proactive upkeep, and adherence to marine rules. By diligently following a rigorous maintenance plan, vessel owners can effectively mitigate the risk of significant failures and ensure optimal performance and safety of their vessels. This proactive approach allows for the early detection and resolution of possible issues before they worsen.

Vessels are significant investments, and appropriate maintenance safeguards this investment by prolonging the vessel's lifespan and ensuring that it continues to function effectively. Vessel owners may optimize maintenance schedules, minimize costs, and assure compliance with regulatory requirements by using effective maintenance techniques such as preventative maintenance and condition-based monitoring (Mr. Marine, Vessel Maintenance, 2024). Adopting a comprehensive strategy for maintenance is crucial for maintaining the vessel's performance and ensuring it stays in peak condition over its entire lifespan.

The benefits of proper maintenance are as follows:

Reduced downtime	Lower Repair Costs	Extended Machinery Life	Safety Enhancement
• Smooth machinery operation • Preventive maintenance reduces malfunctions • Increased fleet productivity	• Preventative maintenance saves money • Early detection prevents major repairs • Cheaper fixes during regular checks	• Prevents wear and premature failures • Avoids expensive replacements • Maximizes machinery value and performance	• Reduces the risk of failures • Protects vessel, cargo, and crew • Creates a safer working environment

Integrating Loss Prevention & Maintenance – A Key to Reduce Claims

Relying solely on maintenance is not sufficient because it does not address all potential risks and inefficiencies. Loss prevention complements maintenance, as it is a proactive strategy that emphasizes the identification and mitigation of risks prior to their development into costly incidents or insurance claims. In the marine industry, where the machinery is intricate and the stakes are high, effective loss prevention can be the deciding factor between a peaceful sailing and a calamitous failure that results in substantial financial loss.

The key aspects of loss prevention include the following measures:

Predictive Maintenance

- **Real-Time Monitoring:** Continuously monitor machinery performance to anticipate failures.
- **Cost Savings:** Helps avoid costly emergency repairs by scheduling maintenance before failures occur.
- **Example:** Royal Caribbean uses GE's SeaStream Insight to detect early signs of engine deterioration, scheduling maintenance during port calls.

Regular Training

- **Up-to-Date Knowledge:** Ensure crew members are trained on the latest safety protocols and operational procedures.
- **Error Reduction:** Minimizes human error, which is a major cause of machinery-related accidents.
- **Example:** ABS emphasizes ongoing training to adapt to evolving regulations and low-carbon shipping practices.

Condition Monitoring

- **Early Issue Detection:** Uses methods like vibration analysis, thermography, and oil analysis to identify potential problems.
- **Preventive Maintenance:** Facilitates timely maintenance, reducing the likelihood of catastrophic failures.
- **Example:** Shell's Prelude FLNG uses condition monitoring to detect gas turbine issues early, preventing expensive shutdowns.

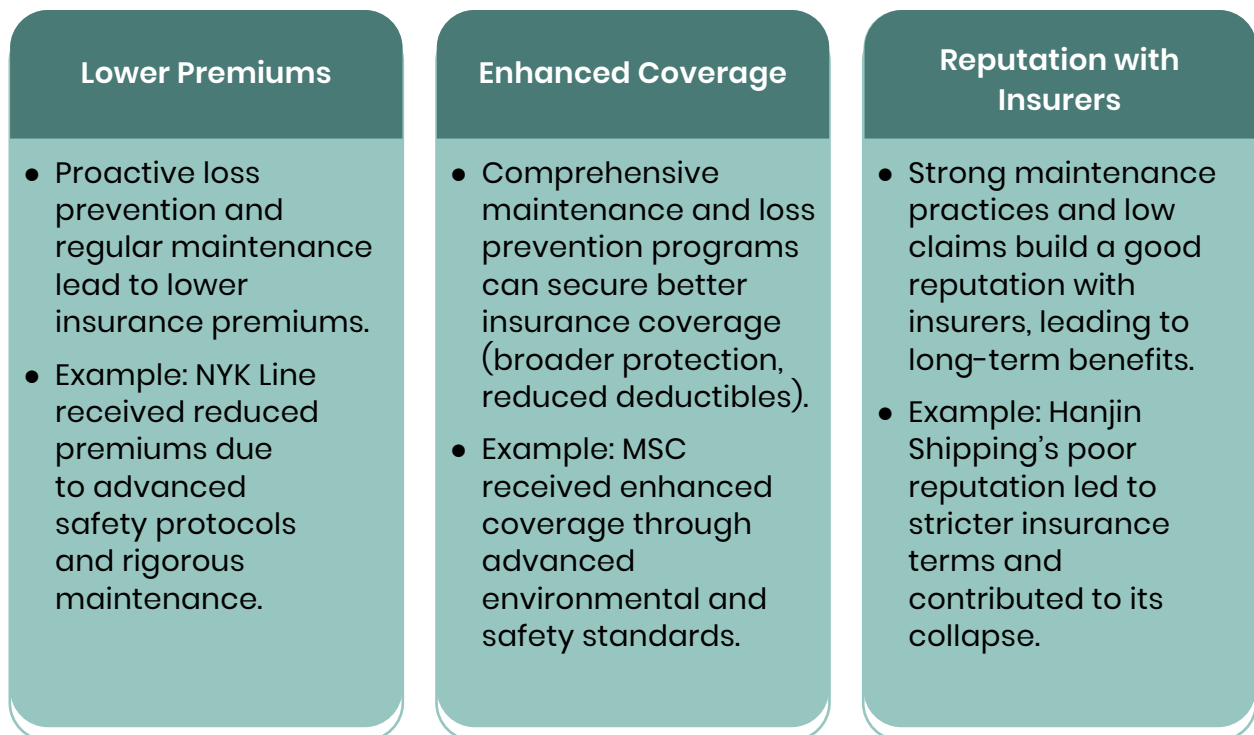
Data Analytics

- **Informed Decision-Making:** Artificial intelligence (AI) and machine learning (ML) analyze real-time data to detect subtle anomalies and inefficiencies.
- **Trend Analysis:** Identifies recurring issues by analyzing historical data, helping to refine maintenance protocols.
- **Predictive Insights:** Data analytics can predict potential failures, allowing for proactive prevention measures.

Enhancing Insurance Terms through Effective Maintenance and Loss Prevention

In the highly regulated and risk-intensive marine industry, vessel operational integrity is critical for safety, efficiency, and insurance terms. Insurance companies evaluate a vessel's risk based on maintenance and loss prevention. Insurers assess a vessel's risk profile by comprehensively analyzing its maintenance practices and loss prevention measures. Insurers perceive vessels that are well-maintained and have a strong history of preventive care as less risky, leading to more favourable insurance terms, including reduced premiums and expanded coverage. This relationship emphasizes the importance of diligent maintenance procedures, as they have a direct impact on the cost-effectiveness of a vessel's operations and its insurability.

The strategies include:



Case Study: Effective Machinery Maintenance and Loss Prevention of Maersk Line

Maersk Line, one of the biggest container shipping firms in the world, has a vast fleet of vessels that it operates all over the world. The firm confronts enormous risks related with machinery failures due to the huge fleet it maintains.

These breakdowns might result in delays to the company's operations and expensive insurance claims. Maersk Line encountered numerous machinery malfunctions during the early 2010s, which resulted in substantial operational delays and insurance claims. Maersk Line developed a thorough maintenance and loss prevention plan focused on marine machinery to help reduce the dangers highlighted by previous incidents, particularly as the business grew its fleet and worked in demanding surroundings.

Maersk Line enhanced its machinery maintenance and loss prevention by implementing the following:-

1. Implementation of Predictive Maintenance:

- a. The concept of predictive maintenance entails the use of sophisticated technology to actively monitor machinery's functionality in real time. Instead of relying on a scheduled maintenance interval or a breakdown event, the implementation of predictive maintenance enables the ongoing evaluation of machinery condition. To achieve this goal, Maersk Line made strategic investments in many essential technologies:
 - i. Vibration analysis: Mechanical components, such as engines and pumps, exhibit vibrations, which the method of vibration analysis quantifies to identify imbalances, misalignments, or signs of wear and tear. The presence of abnormal vibrations often serves as an early indicator of mechanical problems, allowing for prompt intervention before a breakdown occurs.
 - ii. Oil condition monitoring: This involves the examination of the oil used in engines and other machineries, enabling technicians to detect any contaminants or changes in the oil's qualities that may indicate internal deterioration or the existence of metallic particles. This technique has the potential to facilitate the early detection of problems such as bearing failures or gear wear and tear.
 - iii. Thermography: Thermography is a technique that uses infrared cameras to identify and analyze heat distribution patterns inside machines. Unusual heat signatures may be an indicator of electrical failures, friction, or ineffective cooling systems. By identifying these problems early, we can take preventative measures before they cause severe harm or downtime.

2. Regular Crew Training:

- a. The effectiveness of maintenance and loss prevention is significant upon the crew's level of knowledge and proficiency. Maersk Line recognizes the importance of providing comprehensive training to all crew members on the operation and maintenance of machinery on board.

- b. The implementation of training sessions aimed to equip crew members with a thorough understanding of machinery operation, thereby reducing the likelihood of operator errors, a common cause of machinery malfunction.
- c. The training session also included the latest machinery maintenance procedures, providing the team with the requisite expertise to proficiently and appropriately execute regular inspections and maintenance duties.

3. Partnership with Manufacturers:

- a. Maersk Line has developed strong partnership with the companies that provide the machinery and supplies that they use throughout their operations. These partnerships have provided several significant benefits:
 - i. Access to Expertise: Maersk Line diligently collaborated with manufacturers to ensure that their maintenance processes were in accordance with the most up-to-date technical requirements and recommendations. This collaborative effort ensured the execution of all maintenance and repair tasks using optimal methods and authentic parts.
 - ii. Updates on Risks: In the realm of machinery, manufacturers often possess the most current and relevant knowledge pertaining to new risks. Their collaborative relationships provided Maersk Line with regular information about potential vulnerabilities and operational changes, thereby enhancing safety and operational efficiency.

4. Enhanced Condition Monitoring:

- a. Condition monitoring systems exhibit a higher level of sophistication and continuous operation in contrast with traditional maintenance methods. Maersk Line has improved its condition monitoring capabilities by utilizing technologies that continuously check the operational efficiency of critical machinery components.
- b. Real-time data collection involves the placement of sensors on machinery components to gather information on a range of characteristics, including temperature, pressure, and vibration, during dynamic operation. Continuous data acquisition enables prompt identification of any irregularities as they manifest.

- c. The data analysis process involves the use of advanced algorithms to examine the obtained data, with the aim of predicting probable errors by identifying patterns and trends. This facilitates the generation of well-informed recommendations about the optimal timing for maintenance activities.

5. Scheduled Maintenance and Inspections:

- a. The implementation of scheduled maintenance and inspections serves as the fundamental framework for every maintenance program. Taking it a step further, Maersk Line followed a maintenance plan that exceeded all expectations:
 - i. Maersk Line has meticulously considered regulatory mandates and manufacturer guidelines to implement a rigorous schedule for maintenance operations. This schedule upheld regular inspections and maintenance for all machinery components.
 - ii. Maersk Line diligently maintained a comprehensive record of repair operations, ensuring strict adherence to international laws, including those established by the International Maritime Organization (IMO). This paperwork played a vital role in facilitating operational audits and serving insurance-related objectives.

The following are the impacts resulting from the measures taken:

1. Significant Reduction in Machinery-Related Claims:

- a. The successful integration of predictive maintenance and improved condition monitoring initiatives resulted in a significant reduction in machinery-related incidents. Maersk Line documented a notable 20% decrease in insurance claims associated with mechanical malfunctions over a five-year timeframe. The observed decrease may be attributed to the timely identification and resolution of possible problems prior to their escalation into significant failures.
- b. Maersk Line was able to save money because of the decline in claims, which cut down on insurance payments, interruptions to operations, and repair expenses. Maersk's fleet's increased dependability, resulting in fewer mechanical breakdowns, enhanced overall operational performance.

2. Improved Operational Efficiency:

- a. Maersk Line's proactive maintenance strategy produced considerable increases in operational effectiveness. Less unplanned failures meant less downtime for the vessels, which is very vital for a shipping corporation running under strict deadlines. More vessels allow Maersk to consistently meet its delivery targets, resulting in great customer satisfaction.
- b. Enhanced operational efficiency also allowed Maersk to maximize fleet use. Machinery running at maximum capacity allows the business to avoid expensive delays, rerouting, or backup vessel requirements. This improvement not only boosts the company's profitability but also enhances its competitive advantage in the shipping industry.
- c. Delivery on time become more constant, which improved relationships with clients who value dependability. Reduced disruptions resulted in more effective operations, hence improving resource management and profitability.

3. Favourable Insurance Terms

- a. Maersk Line's commitment to thorough maintenance and loss prevention not only improved their operations, but also greatly impacted their relationship with insurance companies. Maersk was able to negotiate better rates for insurance by proving a reduced risk profile resulting from excellent maintenance policies. This included cheaper premiums, as companies understood the lower chance of expensive claims resulting from mechanical failures.
- b. Reduced deductibles for machinery-related claims also reflected insurers' faith in Maersk's fleet maintenance. To further strengthen Maersk's financial situation, more extensive coverage choices were available, covering a wider range of possible hazards at reasonable costs.
- c. Lower premiums and deductibles meant significant cost savings, therefore enhancing the company's financial situation. By covering more ground, Maersk could better control risks and ensure the business's safety against unanticipated occurrences.

4. Strengthened Reputation

- a. The success of Maersk Line's maintenance and loss prevention programs significantly enhanced its reputation within the marine industry. Maersk has proven that proactive maintenance and predictive monitoring can effectively mitigate the risks associated with machinery failures. This reputation was critical for establishing more robust relationships with insurers, who perceived Maersk as a lower-risk client, and consumers, who prioritized safe and reliable operations.
- b. Additionally, new business opportunities were fostered by a strengthened reputation. Clients and partners were increasingly interested in collaborating with Maersk due to its commitment to operational excellence, reliability, and safety. This reputational boost strengthened Maersk's position as a worldwide shipping industry leader.

The Maersk Line case study exemplifies the concrete advantages of allocating resources to marine machinery maintenance and loss prevention. The organization effectively mitigated the likelihood of machinery failures by implementing a proactive strategy that includes predictive maintenance, consistent training, and extensive coordination with manufacturers. Consequently, these factors resulted in a reduction in insurance claims, improved operational efficiency, and more advantageous insurance conditions, thus playing a significant role in the company's sustained prosperity within the fiercely competitive marine industry.



Conclusion

Proper maintenance and loss prevention measures in marine machinery significantly impact insurance premiums and claims. Allianz Global Corporate & Specialty (AGCS) has reported that the number of incidents on large vessels has increased, accounting for 18% of marine claims by value from 2017 to 2021, which is equivalent to approximately €1.65 billion (Commercial Allianz, 2022). This rise in incidents underscores the critical importance of preventive measures such as regular maintenance and crew training to mitigate such risks.

Inflation and the increasing value of vessels have also increased the cost of claims. For instance, the 26% increase in the global merchant fleet's combined value to \$1.2 trillion in 2021 has increased the financial implications of incidents (Actuarial Post, 2022). By decreasing the frequency of machinery failures and the ensuing repair costs, proactive maintenance can assist in preventing these costly claims. These costs have increased due to rising steel, spare parts, and labour prices.

The Journal of Shipping and Trade published research suggesting that proactive loss prevention could potentially reduce the frequency of maritime claims by up to 15% (Carine Dominguez-Péry, 2021). This prevention involves tackling human error via improved training and maintenance standards. This decline in occurrences will result in fewer insurance claims and reduced overall expenses for vessel operators. Industry analysis indicates that incidences such as engine room fires, which are frequently associated with inadequate maintenance, can result in substantial financial losses and increased insurance premiums. Vessel proprietors can achieve improved coverage conditions and reduced insurance costs by employing preventive strategies to mitigate these risks.

These insights emphasize the financial and operational advantages of investing in comprehensive maintenance and loss prevention programs. In addition to ensuring the integrity of their vessels, vessel owners establish a stronger relationship with insurers by prioritizing these endeavours. This leads to better insurance terms and a more sustainable and resilient business operation.

*Prepared By:
Siva Sanggary a/p Sambath*

References

- Norwegian Maritime Authority. (2023). Retrieved from Vessel inspection: <https://www.sdir.no/en/shipping/vessels/vessel-surveys/>
- ABS . (12 6, 2023). Retrieved from ABS Tackles Real-Time Issues in Container Shipping Landscape with Maritime Experts: <https://news.cision.com/american-bureau-of-shipping/r/abs-tackles-real-time-issues-in-container-shipping-landscape-with-maritime-experts,c3941223>
- Actuarial Post. (2022). Retrieved from Key trends in marine insurance claims from fire to inflation: <https://www.actuarialpost.co.uk/article/key-trends-in-marine-insurance-claims-from-fire-to-inflation-21436.htm>
- Andrea Maternová, M. M. (13 10, 2023). Human Error Analysis and Fatality Prediction in Maritime Accidents. Retrieved from MDPI: <https://www.mdpi.com/2077-1312/11/12/2287>
- ATTRI. (n.d.). Retrieved from AI Predictive Maintenance: <https://attri.ai/ai-blueprints/ai-predictive-maintenance>
- Carroll, A. T. (11 8, 2021). Cost Benefit of Implementing Advanced Monitoring and Predictive Maintenance Strategies for Offshore Wind Farms. Retrieved from MDPI: <https://www.mdpi.com/1996-1073/14/16/4922>
- Commercial Allianz. (november, 2022). Retrieved from Global claims trends to watch in marine insurance: <https://commercial.allianz.com/news-and-insights/expert-risk-articles/marine-claims-trends.html>
- Dozuki. (2023). A Comprehensive Guide to Predictive Maintenance in Manufacturing. Retrieved from <https://www.dozuki.com/blog/a-comprehensive-guide-to-predictive-maintenance-in-manufacturing-2023>
- Filipsson, F. (5 6, 2024). AI for Predictive Maintenance: Reducing Downtime and Costs. Retrieved from <https://redresscompliance.com/ai-predictive-maintenance/>
- Floren, P. (14 3, 2016). GE. Retrieved from GE Brings Latest Technology Innovations to Build Safer, Cleaner and More Efficient Cruise Vessels: <https://www.ge.com/news/press-releases/ge-brings-latest-technology-innovations-build-safer-cleaner-and-more-efficient>
- Floren, P. (9 5, 2016). GE Enters the Container Ship Industry, Equipping Maersk Line's 2nd Generation Triple-E Vessels with Technology, Improving Fuel Efficiency and Operational Flexibility. Retrieved from GE: <https://www.ge.com/news/press-releases/ge-enters-container-ship-industry-equipping-maersk-lines-2nd-generation-triple-e>
- Mr Marine – Vessel Maintenance. (12 1, 2024). Retrieved from Mr Marine: <https://mr-marinegroup.com/vessel-maintenance/>
- MSC. (2023). Retrieved from MSC Sustainability: <https://www.msc.com/sustainability>
- NYK Group. (2020). Retrieved from <https://www.nyk.com/english/>
- Shell Global. (2018). Retrieved from Floating LNG: <https://www.shell.com/what-we-do/oil-and-natural-gas/liquefied-natural-gas-lng/floating-lng.html>
- Times, F. (2016). The Fall of Hanjin Shipping: Lessons for the Maritime Industry.
- Unit, U. C. (24 11, 2022). The UNCTAD Review of Maritime Transport 2022. Retrieved from Unctad: <https://unctad.org/press-material/unctad-review-maritime-transport-2022>



OUR HEROES, ABANG BOMBA SHIELD US, BUT WHO SHIELDS THEM?

Our Hero

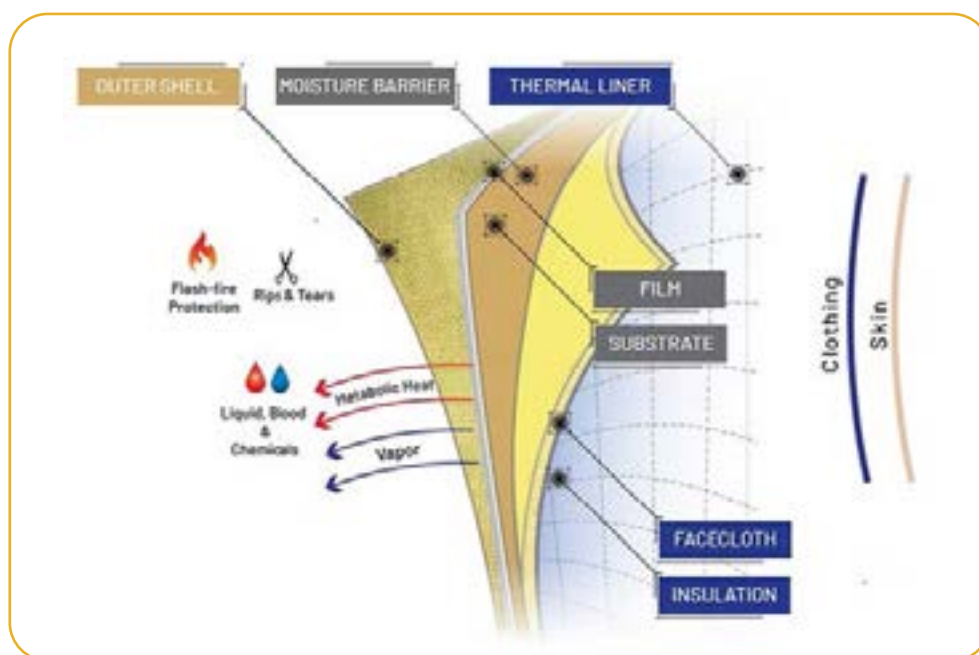
Firefighters, commonly known as 'Abang Bomba' in Malaysia, are our honourable unsung heroes who have been bravely serving the nation for centuries. "Abang Bomba" with a team of dedicated firefighters will immediately come to the rescue after the automatic fire alarm system triggered on fire which could then alert the fire brigade via a central alarm monitoring station.

Have you ever wondered how a firefighter's uniform protects them from extreme heat that could cause fatal burns? Bunker gear designs must also consider garment interfaces (i.e., sleeve and glove, pants, boot, collar, hood and coat hem and waistline).

The thermal protection is provided by the firefighting fabric systems with different layers under high-level thermal temperature range of 800°C-1000°C. The purpose of these fabric systems is to provide actual protection against burn injuries like garments worn by industrial workers, fire fighters and military personnel.

Hero The firefighting fabric thermal protection consists of outer thermal reflective layer (outer shell), thermal storage layer (moisture barrier), thermal liner, and inner comfort layer all of which were laminated together.

The Function of Every Layers



Design Source: PBI Performance Products

Outer Shell

Protect from the thermal burns, cuts, abrasion.

Moisture Barrier

Keeps the water and the moisture chemical from coming through.

Thermal Liner

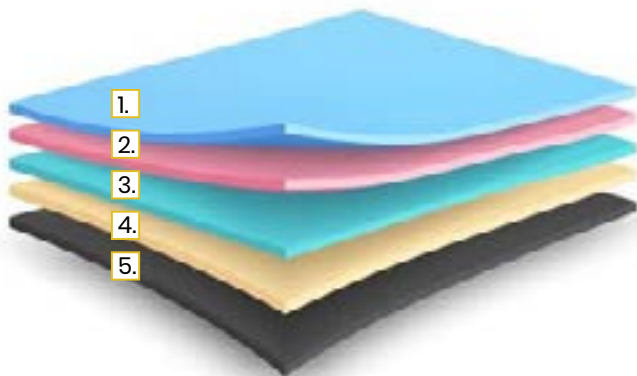
Last line of defense to encounter real hostile environments when fighting a structural fire.

Materials for Advance Design

The advance design, methodology, and approach of the fabric system consist of glass with aluminum foil as an outer layer, non-woven basalt, and non-woven glass fabric containing NaCl-MgCl₂ (a combination of sodium chloride (NaCl) and magnesium chloride (MgCl₂) and Galactitol phase change materials (PCM) which simulate multilayer firefighter protective clothing system.

Thermal protective performance tests were applied for thermal analysis and used to quantify the insulating characteristics of fabrics under conditions of flash-over temperature. The firefighting multilayer protective fabric surface was characterized using the UV-Vis-NIR (ultraviolet-visible-near infrared) spectrophotometer.

The clothing shows good thermal insulation and high-temperature drop during flash over the environment and avoids second-degree burn. The current PCM works in high temperatures, with high efficiency which provides people with better protection against fire exposure and increases the duration time which was estimated to be more than five minutes to prevent burn injuries.



1. Glass with aluminium foil
2. First stage (PCM)
3. Non-woven basalt fabric
4. Second stage (PCM)
5. Non-woven glass fabric



The Process of Making Firefighter's Uniform

Modern firefighters wear advanced protective gear that greatly reduces burn-related fatalities. Their jackets, made from over 90 precisely cut parts, feature three layers, including PBI (Polybenzimidazole), which withstands temperatures up to 648°C. A machine seals the moisture barrier's seams using heat and pressure, allowing perspiration to escape while blocking harmful liquids like battery acid and hydraulic fluid.

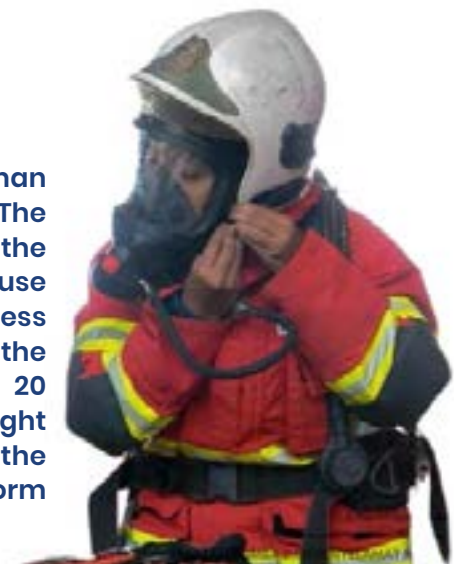


Source: JBPM Negeri Sembilan

This synthetic fabric withstands heat up to 426°C. Heat-resistant tape and thread reinforce the cuffs, hems, and panels, leaving the neck unattached. Orange and silver stripes improve visibility—orange for day light and silver for night or smoke. A fabric strip creates a moisture barrier at the front to block water. The front and back panels are sewn together, reinforcing seams with five stitches at the shoulders to support an 11kg air tank. A heat-resistant plastic zipper is sewn onto the right front panel.

A 1.8-meter strap around the armpits helps drag an injured firefighter to safety. The inner layers snap onto the outer shell, with four heat-resistant snaps on each cuff. The 10 cm collar unfolds to cover the neck up to the helmet. Fully assembled, the jacket weighs just over two kilograms. The jacket is tested for burn resistance by exposing its outer layer to a 1093°C flame from a gas burner to measure the time before a second-degree burn occurs.

A heat sensor mimics human skin sensitivity to heat. The material fails the test if the transferred heat would cause second degree burns in less than 17.5 seconds. Finally, the uniform is showered for 20 minutes to test its watertight seal. Just one wet spot on the bodysuit and the uniform fails inspection.



Malaysia Statistic Source

Here are the main highlights from the graph on Emergency Call Statistics:

1. Total Emergency Calls:

- 2018: 110,150 calls
- 2021: Peak of 167,989 calls
- 2022: Declined to 126,779 calls

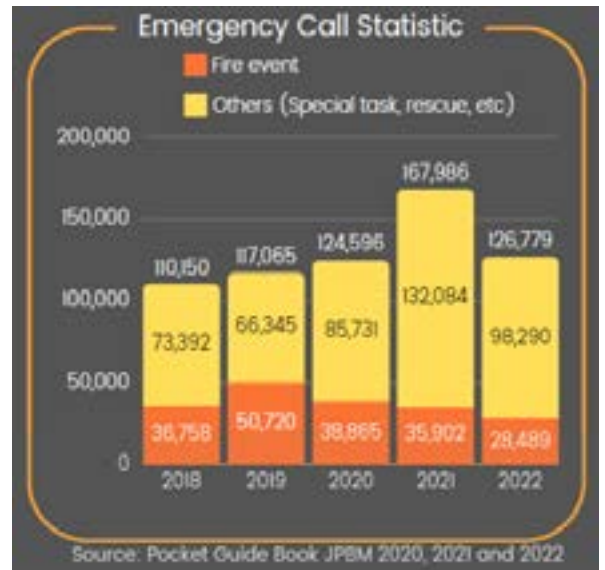
2. Fire-Related Incidents:

- 2019: Highest at 50,720 cases
- 2022: Decreased to 28,489 cases

3. Other Emergency Cases :

(Special Tasks and Rescues)

- 2021: Significant rise to 132,084 cases
- 2022: Dropped to 98,290 cases



EMERGENCY NUMBER: GENERAL **999** | MOBILE **112**

Does Insurance Company Cover Abang Bomba

Bomba Insurance Coverage for Firefighters in Malaysia

Government Coverage

- BOMBA arranges insurance for its firefighters, including life, accident, and health insurance.
- Group insurance schemes for civil servants cover accidents, injuries, or fatalities on duty.
- Coverage is through government-approved providers, with premiums paid by the government.

Individual Coverage

- Firefighters can get additional personal insurance from private companies.
- Options include personal accident insurance, critical illness insurance, etc.

Takaful

- Some firefighters prefer Takaful policies, which follow Islamic principles.
- Available from takaful providers in Malaysia

Accident & Disability Insurance

- Specialized policies cover injuries sustained on duty.
- Can be part of the group plan or taken out individually.

Supplementary Coverage

- Firefighters may option for extra coverage for themselves and their families,
- like life or health insurance.

Conclusion

To conclude, Firefighters, also well known as "Abang Bomba" in Malaysia, play a crucial role in protecting lives and property, often risking their own safety in the line of duty. Their protective gear, designed with advanced materials and multilayer fabric systems, provides essential thermal protection against extreme temperatures, ensuring they can withstand the harsh conditions of fire emergencies.

Beyond their physical protection, Malaysian firefighters are also supported by various insurance schemes, both government-sponsored and private. These policies provide financial security in cases of accidents, injuries, or fatalities, ensuring that firefighters and their families receive the necessary support. The availability of Takaful insurance further expands their options, catering to those who prefer coverage aligned with Islamic principles.

With these measures in place, firefighters are not only equipped to handle emergencies but also assured of financial protection, reinforcing their invaluable contributions as Malaysia's unsung heroes.

Prepared By:
Amar Johan Bin Ishak
Technical Services Department
Market Service Division

References

Ali, A. H. M., & Yu, W. (2014). Thermal protective performance of multilayer firefighting fabric. *International Journal of Clothing Science and Technology*.

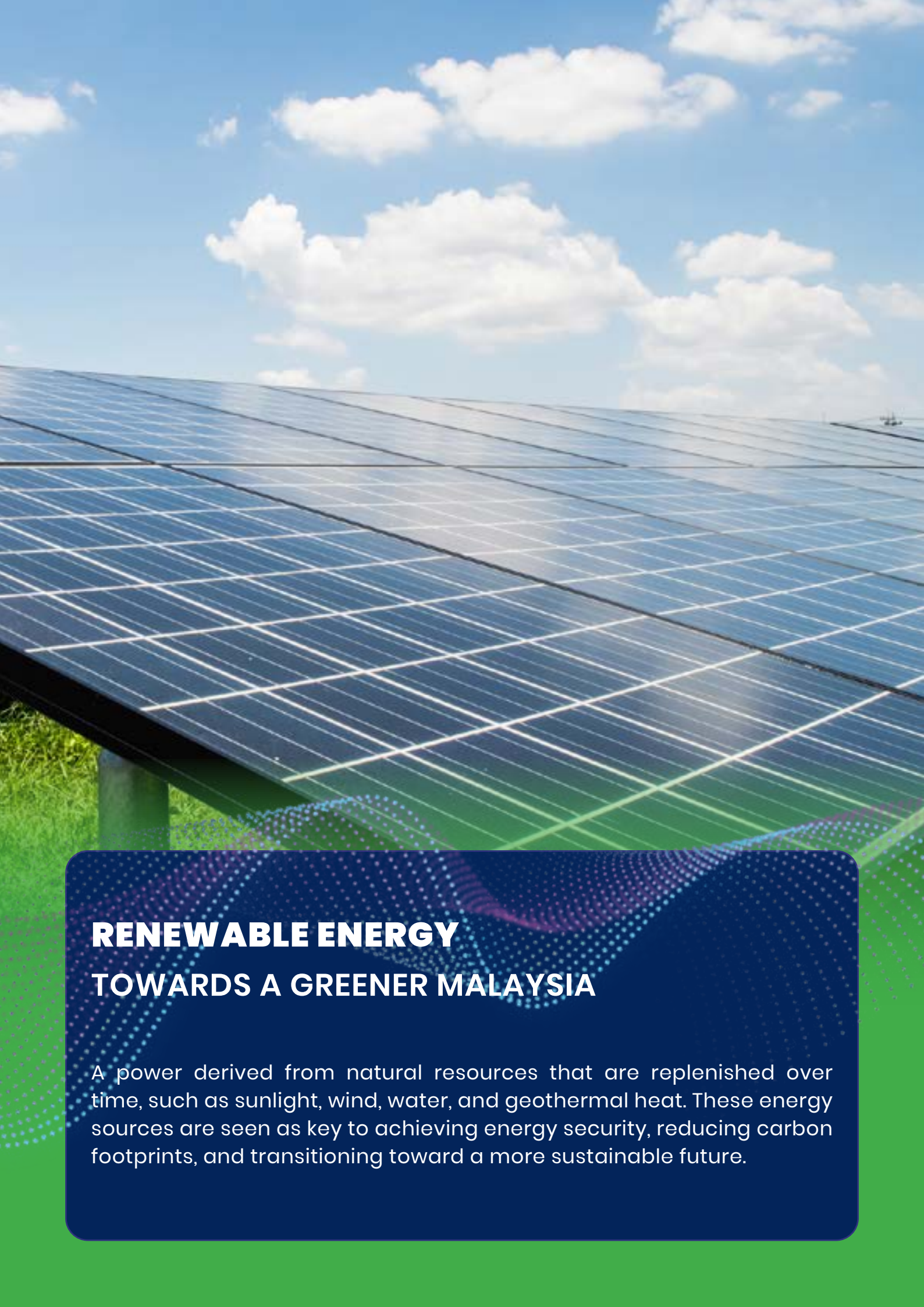
McQuerry, M., Kwon, C., & Johnson, H. (2019). A critical review of female firefighter protective clothing and equipment workplace challenges. *Research Journal of Textile and Apparel*.

How Firefighters Uniform is made, narrated by Karen Taylor. Source from:
https://www.youtube.com/watch?v=ZQRMEAwOGzE&a_b_channel=KarenTraylor Volunteer
Firefighter & First Responder Insurance. (2017).

Retrieved from The Hartford: <https://www.thehartford.com/group-benefits-producers/volunteer-firefighter-first-responder-insurance>
Malaysia Gazette. (2019, May 25).

6,000 baju kalis api bomba kini selamat dipakai. *Malaysia Gazette*. <https://malaysiagazette.com/2019/05/25/6000-baju-kalis-api-bomba-kini-selamat-dipakai/>
Jabatan Bomba dan Penyelamat Malaysia. (2022, December).

Pocket guide book
(December 2022 ed.). Malaysian Fire and Rescue Department.
<https://www.bomba.gov.my/wp-content/uploads/2023/04/POCKET-GUIDE-BOOK-DISEMBER-2022.pdf>



RENEWABLE ENERGY TOWARDS A GREENER MALAYSIA

A power derived from natural resources that are replenished over time, such as sunlight, wind, water, and geothermal heat. These energy sources are seen as key to achieving energy security, reducing carbon footprints, and transitioning toward a more sustainable future.

Type Of Renewable Energy In Malaysia

Source: Malaysia Renewable Roadmap (SEDA Malaysia, 2021)

1. Solar Energy

A Renewable Energy (RE) source that harnesses energy from the sun. May be captured in two ways:

- Photovoltaic (PV) solar panels, which convert sunlight directly into electricity.
- Solar thermal systems, which capture heat from the sun to generate steam or hot air for heating and power generation.

2. Biomass

A renewable, sustainable source of energy that comes from plants and animals. It's made up of chemical building blocks like carbon and hydrogen.



3. Biogas

- Organic materials (plant and animal products) are broken down by bacteria in an oxygen-free environment.
- The digestion recycles these organic materials, turning them into biogas, which contains both energy (gas), and valuable soil products (liquids and solids).

4. Hydropower

A renewable energy source that harnesses the kinetic and potential energy of flowing or falling water to generate electricity.



5. Geothermal

A renewable, clean, and inexhaustible energy obtained by harnessing the heat of the Earth's interior stored in rocks, soils, and groundwater.

Fossil fuels still dominate over **90%** of Malaysia's energy landscape?

- Coal majored at **36.8%**
- Oil comes in second at **35.7%**
- Gas at just **19.4%**.

Source: Energy Malaysia, Vol. 25 (2024)

Government Scheme On Renewable Energy

Source: Malaysia Renewable Roadmap (SEDA Malaysia, 2021)

FEED-IN-TARIFF (FIT)- SOLAR

FIT Solar discontinued in 2017 & replaced by LSS, NEM, SELCO

Applies only in Peninsular Malaysia and Sabah.

Tariff rate: MYR 0.50 – 1.77/kWh

System size: 4kW – 30 MW

Tenure: 21 years

LARGE-SCALE SOLAR (LSS)

LSS is a competitive bidding program by the Energy Commission to reduce the Levelized Cost of Electricity (LCOE) for large scale solar photovoltaic plant development.

Applies only in Peninsular Malaysia and Sabah.

SOLAR NET ENERGY METERING (NEM)

Implementation of Virtual Net Metering (VNM) allowing excess energy to be exported to designated premises under wholly owned subsidiary company.

Applies only in Peninsular Malaysia.

Tariff rate: Based on consumer's retail tariff

System size: Up to 5 MW per applicant, subject to respective sectors

Tenure: 10 years (one to – one offset)

SOLAR SELF-CONSUMPTION (SELCO)

SELCO replaced NEM in Sabah starting 2019.

Tariff rate: Tariff not applicable for SELCO

System size: 75% of max demand / 60% of fuse rating

Tenure: No tenure period

CORPORATE GREEN POWER PROGRAMME (CGPP)

Corporate Consumer is only allowed to have one Corporate Green Power Programme (CGPP) with a Solar Power Producer but a Solar Power Producer is no longer bound to maximum number amount of Corporate Consumers provided that they are within their export capacity.

Tariff rate: Follow system marginal price under NEDA rules.

System size: Up to 30 MW

Tenure: 21 years

FEED-IN-TARIFF (FIT)- BIOMASS

Includes agriculture residues: palm oil and rice husk and straw.

Power Purchase Agreement (PPA) revised to 21 years from 16 years in December 2019.

Tariff rate: MYR 0.27 – 0.31/kWh

System size: Up to 30 MW

Tenure: 21 years

FEED-IN-TARIFF (FIT)- BIOGAS

In 2019, Power Purchase Agreement (PPA) tenure period extended from 16 years to 21 years.

FiT rate offered for agriculture waste and land fill waste.

Tariff rate: MYR 0.27 – 0.32/kWh

System size: Up to 30 MW

Tenure: 21 years

FEED-IN-TARIFF (FIT) - WASTE-TO-ENERGY (WTE)

Effective 2019 new WTE projects who wishes to apply for FiT can apply under Biomass FiT (without the use of solid waste as fuel source bonuses).

Government implemented auction/bidding system for WTE projects started in 2020.

Tariff rate: MYR 0.27 – 0.31/kWh

System size: Up to 30 MW

Tenure: 21 years

FEED-IN-TARIFF (FIT) - SMALL HYDRO

No depreciation rates due to long gestation period.

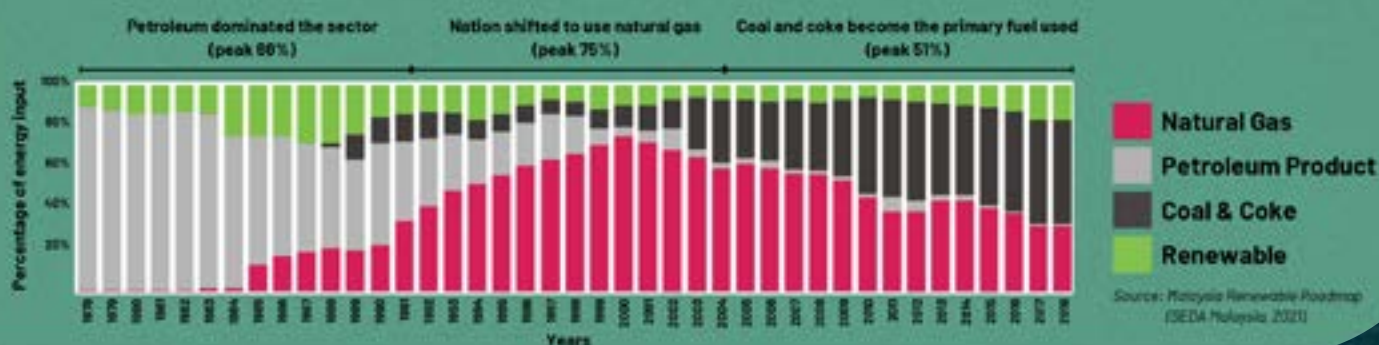
FiT rate for low head and high head introduced in 2019.

Tariff rate: MYR 0.23 – 0.29/kWh

System size: Up to 30 MW

Tenure: 21 years

ENERGY INPUT IN MALAYSIA POWER STATION, 1978 – 2018



CURRENT POWER GENERATION AS AT 2023

25,862
MW

Peninsular

1,180
MW

Sabah

4,640
MW

Sarawak

Source: Energy Malaysia, Vol. 25 (2024); Sabah Energy Roadmap and Master Plan 2040; 2022 Annual & Sustainability Report (Sarawak Energy Berhad)

TOTAL POWER GENERATION BY TYPE

Hydro: 4.6%
Solar: 1.6%
Others: 0.2%

As of end of 2023
*Covers Peninsular Malaysia only

Gas: 36.5%
Coal: 57.1%

Source: Energy Malaysia, Vol. 25 (2024)

Re Capacity Target

In 2023, renewable energy (RE) contributed 8% to Malaysia's electricity generation, up from 7.94% in 2021. Following the National Energy Transition Roadmap (NETR) introduction in August 2024, the government set ambitious RE capacity targets to accelerate the transition to renewable energy.

31% 40% 70%

by 2025 by 2035 by 2050



Year	Solar (MW)	Biomass (MW)	Biogas (MW)	Large Hydro (MW)	Small Hydro (MW)	Geothermal (MW)
by 2025	4,706	862	333	5,062	1,153	0
by 2035	7,280	996	406	8,062	1,219	30

Source: Malaysia Renewable Roadmap (SEDA Malaysia, 2021)

References

Malaysia Renewable Energy Roadmap Pathway Towards Low Carbon Energy System Report. (n.d.). SEDA Malaysia 2021. https://www.seda.gov.my/reportal/wp-content/uploads/2022/01/MyRER_webVer2.pdf.

Sarawak Energy – 2022 Annual & Sustainability Report. (n.d.). Sarawak Energy. <https://www.sarawakenergy.com/assets/pdf/SarawakEnergy-ARSR2022.pdf>.

Energy Commission – Energy Malaysia, Volume 25, 2024 (2024). <https://www.st.gov.my/publ/EM/vol25.pdf> Sabah Economic Planning Unit. (2023).

Sabah energy roadmap and master plan 2040 (SE-RAMP 2040). Economic Planning Unit, Sabah. <https://ecos.gov.my/sites/default/files/uploads/downloads/2023-09/SABAH%20ENERGY%20ROADMAP%20AND%20MASTER%20PLAN%202040%20%28SE-RAMP%202040%29.pdf> 1.2.3.4.