PRESS RELEASE

Cygienic.com Supports Proactive Cyber Insurance to Close the Small Business Cybersecurity Gap.

*Cygienic's insurability assessment results found that **42%** of small business websites and proprietary web-apps would require cyber remediation prior to being insurable.*

SINGAPORE – 15/08/26 – Cygienic assessed the cyber insurability readiness of 1,200 companies across six major ASEAN markets - Singapore, Malaysia, Indonesia, the Philippines, Thailand, and Vietnam. The findings were striking: while larger enterprises generally demonstrated stronger cyber resilience, SMEs consistently lagged behind on most key security controls, highlighting a significant gap between eligibility for cyber insurance and sufficient resilience to cyberattacks.

The results suggest that cyber insurance alone cannot close the SME cybersecurity gap. Insurability should be viewed as the starting point for improvement - not the finish line - with insurers, brokers, and businesses working together to identify cyber risk weaknesses, improve security posture, and then continuously monitor cyber risks.

Cyber Insurability Readiness Test

• ASEAN Large Corporation x600 Insurability 71% | **Remediation required 29%**
• ASEAN SME Companies x 600 Insurability 58% | **Remediation required 42%**

CyberIQ Readiness Scope: Email Security, Web Security, Vulnerabilities, Host Reputation, Data Privacy, Open Ports, PCQ.

The results indicate that large corporations outperformed SMEs with a 70% insurability readiness compared to 58%, leaving 29% and 42% requiring remediation, respectively. However, these figures highlight a critical cyber gap regardless of company size.

"The opportunity here is to stop treating cyber insurance as a pass-or-fail transaction," said Barnaby Grosvenor, Founder and CEO of Cygienic. ***"For SMEs that fall short today, the answer does not have to be 'no'. Brokers can help identify the gaps, establish a remediation pathway and demonstrate measurable improvement. Once insured, continuous monitoring can help ensure that the risk does not simply deteriorate again."***

Proactive Cyber Insurance changes the game. By combining continuous risk management, real-time threat monitoring, and insurance coverage, companies receive a complete, active security dynamic rather than a passive piece of paper.

The question for insurance brokers, therefore, should not simply be: "*Is this SME secure enough to insure?*" It should be: ***"What does this SME need to improve to become insurable – and how can we prove that it has improved?"***

The SME Resilience Gap

While CyberIQ testing showed large enterprises leading across most technical controls, SMEs delivered a stark surprise: SMEs outperformed enterprise corporations in email credential exposure, with 760 Vs 6066 email credentials found in the Dark web.

This crucial takeaway proves that company size alone does not dictate cyber hygiene. However, the overall resilience gap remains an urgent challenge. SMEs operate with tighter budgets, scarce technical resources, and little capacity for continuous external monitoring, leaving them dangerously vulnerable to expanding cyber threats.

From Insurance Barrier to Improvement Pathway

Cyber insurance must evolve from a hurdle into an operational upgrade.
Rather than treating underwriting as a binary rejection, forward-thinking brokers and insurers are using risk intelligence to diagnose weaknesses and hand SMEs an execution roadmap.

The journey becomes a continuous loop: **Cyber insurance → SME resilience gap → remediation → insurability → continuous monitoring.**

This fundamentally rewrites the relationship between businesses and insurers. The era of filling out a static questionnaire and praying for approval is over. Instead, a true partnership is formed - continuously monitoring and dismantling risks for the lifetime of the policy.

• For SMEs: A practical blueprint to prove ongoing insurability, harden defences, and turn risk into resilience.
• For Brokers & Insurers: greater portfolio visibility, improved risk intelligence and an opportunity to engage underserved SMEs before and throughout the policy lifecycle.

Turning the Cyber-Resilience Gap into an Opportunity

Falling behind in cybersecurity shouldn't mean getting locked out of the insurance market. For ASEAN SMEs, initial risk exposure isn't a dead end - it is the starting point for a measurable journey to resilience, protection, and long-term insurability.

SMEs don't need to wait until they are perfectly secure to begin their insurance journey. They need a measurable path to becoming more resilient - and a mechanism for demonstrating that improvement.

End.

Methodology & Scope

1. Sample Breakdown

The study evaluated **1,200 organizations** across six primary ASEAN markets (Singapore, Malaysia, Indonesia, Philippines, Thailand, and Vietnam).

Category	Sample Size	Qualification Criteria	Industry Coverage
Large Corporations	600	Mainboard-listed companies	Multi-sector representation
SMEs	600	< 100 employees **and** < US$5M annual revenue	Multi-sector representation
Total Evaluated	**1,200**	—	—

2. Technical Scope & Limitations

- **Assessment Focus:** Purely non-intrusive **external risk posture** evaluated via each organization's primary domain (TLD only).
- **Boundaries:** The assessment does **not** measure internal security posture, including:
    - Private/internal networks and databases
    - Employee end-user devices
    - Unlinked internal applications.
    - Behind-the-firewall security controls

Key Findings

- **Size Matters:** Large corporations outperformed SMEs across nearly every measured category, reflecting greater access to dedicated security resources, specialist expertise, and formal risk management.
- **Widespread Exposure:** Both tiers exposed exploitable weaknesses through public-facing infrastructure.
- **Basic Hygiene Failures:** Both tiers struggled with basic configurations – for example, 12-15% of websites had security vulnerabilities, and average web security grades landed at a 'D' across the board.
- **The AI Multiplier:** As agentic AI automates the cyber kill chain at machine speed, exposed attack surfaces that once went unnoticed can now be discovered and exploited systematically.

Cyber Insurance Readiness Results

Cyber Resilience Test	ASEAN Large Corp	ASEAN SMEs
Cyber Risk Grade A	[33%]	[22%]
Cyber Risk Grade B	[38%]	[36%]
Cyber Risk Grade C	[19%]	[29%]
Cyber Risk Grade D	[9%]	[11.3%]
Cyber Risk Grade E	[1%]	[1.5%]
Vulnerable Websites	[12%]	[15%]
Bad Host Reputation	[7%]	[12%]
Email Credentials Found	[6066]	[760]
High-Risk Open Port Services	[19%]	[24%]
Quantum SSL Ready Failed	[54%]	[54%]
AI Services Running	[8%]	[4%]
Email SPF Protection Off	[13%]	[25%]
Web Security Grade A–D	[D]	[D]

ASEAN Cyber Insurance Readiness Results

CYBERIQ TEST	SG MAIN	SG SME	TH MAIN	TH SME	VT MAIN	VT SME	MY MAIN	MY SME	PH MAIN	PH SME	IND MAIN	IND SME	TOTAL	MAIN TOTAL	SME TOTAL	Total % 600	Total % 600
A	31	21	41	20	36	15	27	19	37	21	29	38	335	201	134	33.5	22.3
B	38	37	28	26	43	35	43	40	31	37	42	40	440	225	215	37.5	35.8
C	17	29	18	37	15	37	18	30	28	29	19	12	289	115	174	19.2	29.0
D	14	11	12	16	6	10	11	11	4	11	9	9	124	56	68	9.3	11.3
E	0	2	1	1	0	3	1	0	0	2	1	1	12	3	9	0.5	1.5
	100	100	100	100	100	100	100	100	100	100	100	100	1200	600	600		
Email Breach	920	74	1167	166	2145	187	702	108	712	102	420	133	6836	6066	770	6066.0	770.0
Host Rep	8	28	5	10	2	4	7	14	7	11	12	7	115	41	74	6.8	12.3
Vulnerability	15	13	17	26	14	23	12	15	7	5	8	11	166	73	93	12.2	15.5
Quantum Ready	58	47	38	49	73	76	55	41	52	79	47	34	649	323	326	53.8	54.3
AI Services	10	1	11	11	1	1	11	9	1	0	11	0	67	45	22	7.5	3.7
Ports Open	19	22	30	36	16	30	24	32	10	13	17	12	261	116	145	19.3	24.2
Email SPF	10	12	13	14	6	31	9	15	23	64	15	16	228	76	152	12.7	25.3
Web security grade	D	D	C	D	D	D	D	D	D	D	D	D	0	D	D	D	D

End.