

TARIKH	ISNIN, 9 SEPTEMBER 2024
AKHBAR	THE STAR
TAJUK ARTIKEL	GRAPPLING WITH DIGITAL THEFT
M/S	8 – 9
BIDANG	MANAGEMENT
KATA KUNCI	MANAGEMENT

8 Nation

THE STAR, MONDAY 9 SEPTEMBER 2024

By ZAIDI AZMI

GRAPPLING WITH DIGITAL THEFT

Malaysia finds itself at a critical juncture as it charts its way into the turbulent waters of digital piracy

NOT long ago, Malaysia claimed the notorious title of being number one in digital piracy incidence for two consecutive years.

Yet, in an unexpected twist, the South-East Asian nation has now slipped to fifth place.

This intriguing fall was revealed in a survey by Asia Video Industry Association (Avia), which saw Vietnam leading the notorious race among the eight Asian countries surveyed – with a staggering 71% video piracy incidence.

The Philippines was a close second at 70%, Indonesia came in third at 62%, followed by Thailand at 61%, Malaysia at 59%, Hong Kong at 57%, Taiwan at 50% and Singapore at 40%.

Avia's Coalition Against Piracy general manager Matthew Cheetham says Malaysia's latest ranking was largely due to a surge of piracy incidence in the preceding top four countries.

"It was due to the process at play and Malaysia did well. The blocking regime was pretty good, although it seemed to slow down a little bit towards the end of 2022, and last year it started to get a little better."

"There were also criminal actions that were undertaken last year. I think that would have impacted it but, in other countries, you saw a surge, particularly in Vietnam and the Philippines," says Cheetham.

Interestingly, Avia's findings also illustrated a downward trend of video piracy incidence in Malaysia, dwindling from 61% in 2022 to 60% in 2023, and further to 59% in 2024.

Nonetheless, despite this positive decline, Malaysia is still facing significant hurdles in rooting out video piracy.

In fact, in March, the media and entertainment industry was jolted by the discovery of a long-standing digital piracy syndicate, which had been operating for years with seeming impunity.

However, despite the police dismantling the syndicate, there has been no news of its prosecution to date.

Risky tango with K-drama and digital piracy

Surprisingly, it was also revealed that in Malaysia it is the womenfolk who have been driving the consumption of pirated content in 2024.

In fact, Malaysian women make up 54% of pirated content consumers compared to their male counterparts at 55%.

While Avia's survey did not specify the genre of the illicit video content consumed by women in the country, Cheetham believes that K-dramas were highly probable.

"Having worked on this for a very long time, I know how popular K-dramas are when it comes to being pirated but, to be fair, this is my assumption because the question did not ask, 'Do you watch K-dramas?'" says Cheetham.

Like the rest of the surveyed countries, social media and messaging platforms were the most popular gateway used by Malaysians to access pirated content, with Facebook and Telegram sharing the top spot, at 44%.

TikTok came in second place at 36%, followed by WhatsApp at 33%, Instagram at 28% and WeChat at 18%.

Battling digital buccaneers

As Irredo's cyber services vice president and the Audiovisual Anti-Piracy Alliance (AAPA) co-president, Mark Mulready has been standing at the forefront of the war against digital piracy.

His more-than-35-years-worth of insights on digital piracy reflects his hard-won expertise and experience.

"This battle against digital piracy is like playing an endless game of cat-and-mouse," he says, illustrating the ongoing cycle of security measures and exploitation in the fight against online content theft.

As technology evolves, so do the methods used by those seeking to undermine it.

"Nowadays, many are grappling with the complexities of over-the-top (OTT) streaming services," he adds.

Initially, the primary focus was on building platforms and

attracting users. Security was an afterthought, but as these platforms grew, so did the realisation that robust security measures were essential.

"We had to ensure that only legitimate users could access the platform," Mulready explains.

Digital pirates, he adds, continually found new ways to exploit vulnerabilities, prompting swift countermeasures.

"One such instance was when watermarking – embedding visible overlays into content to trace its origin – was circumvented. Pirates quickly adapted, manipulating images to evade detection," says Mulready.

Expectedly, the use of artificial intelligence (AI) was also adopted by both sides.

"We're using AI to build models to detect those anomalies, the pirates have worked out what we're doing and they are also using AI to hide themselves from our detection."

"This is the new cat-and-mouse game – one that is happening in the OTT distribution," says Mulready.

Commoditisation of digital piracy

Digital piracy continues to loom large as it has become extremely lucrative – thus, too tempting for unscrupulous quarters to resist.

Last year, the AAPA reported

that in 2021, the estimated annual global revenue of video piracy stood at US\$2.34bil (RM10.25bil).

"Piracy is now a service and a highly commoditised one," Mulready asserts.

"Anyone with minimal technical know-how can easily become resellers by obtaining access to pirate platforms and selling subscriptions."

This unsettling democratisation of piracy meant that even teenagers, equipped with just a computer, could sell pirated content from the comfort of their bedroom.

To the unfamiliar, piracy services generate revenue through advertising, donations, subscription fees, selling user data and affiliate marketing.

These illicit revenue streams have robbed the creative industries, pay TV companies and tax authorities of legitimate earnings.

For example, a 2016 study by the Tepper School of Business and Heinz College of Carnegie Mellon University in Pennsylvania in the US, discovered that movie piracy can cannibalise up to US\$1.3bil (RM5.69bil) in potential box-office revenues annually.

Delaying the inevitable loss

At a glance, digital piracy has become so rampant and widespread that the ongoing war

Regional anti-piracy measures

MALAYSIA

Challenges
New offences related to copyright infringement.

Outcomes

1. Strengthened enforcement powers, creation of offences for manufacturing, importing, selling streaming technology.
2. Increased enforcement against the selling and distribution of ISOs, pirate apps, other criminal activity on these ISOs.

Regulators / Collaborative Parties

1. Malaysian Communications and Multimedia Commission (MCMC)
2. Royal Malaysian Police (PDRM)
3. Ministry of Domestic Trade and Cost of Living (KPDN)
4. Content Forum Malaysia (CFM)

HONG KONG

Challenges
Introduction of Copyright (Amendment) Bill 2022.

Outcomes

1. Proposed exclusive technology-neutral communication right and criminal sanctions.
2. Additional statutory factors for awarding damages in civil cases.
3. Safe harbor provisions for online service providers introduced.

Regulators / Collaborative Parties

1. Customs and Excise Department
2. Hong Kong Coalition for Intellectual Property Rights (HKCIPR)
3. Hong Kong Motion Picture Industry Association (MPA)

CHINA

Challenges
Responding to copyright infringement lawsuits.

Outcomes

1. Third Amendment increases damages, introduces punitive measures.
2. Authorities can impose fines proportionate to illegal business turnover.
3. Increased damages to deter infringement.

Regulators / Collaborative Parties

1. National Copyright Administration (NCA)
2. Cyberspace Administration of China (CAC)
3. China Audio-Video Copyright Association (CAVCA)
4. Internet Society of China (ISC)

INDONESIA

Challenges
Reduction in piracy traffic but still on U.S. Priority Watch List.

Outcomes

1. Site blocking measures leading to 75% reduction.
2. A total of 3,500++ domains blacklisted.

Regulators / Collaborative Parties

1. Ministry of Communication and Informatics (Kominfo)
2. Indonesian National Police
3. Indonesian Content Providers Association

SINGAPORE

Challenges
Difficulty enforcing rights against sellers of hardware, software, and services for unauthorized content.

Outcomes

1. Singapore Copyright Act 2021 introduces civil and criminal liability on commercial dealers.
2. Targets commercial profits off devices and services facilitating unauthorized access.

Regulators / Collaborative Parties

1. Infocom Media Development Authority (IMDA)
2. Singapore Police Force (SPF)
3. Coalition Against Piracy (CAP)

THAILAND

Challenges
New takedown procedure under Thai Copyright Act (No.6) B.E. 2565 2022

Outcomes

1. Exemption for certain service providers, simplified notice and takedown process.
2. Takedown notice replaces the need for a court order.

Regulators / Collaborative Parties

1. Department of Intellectual Property (DIP)
2. Royal Thai Police (RTP)
3. Thai Entertainment Content Trade Association (TECTA)

PHILIPPINES

Challenges
Pending Online Infringement Bill; increasing local piracy.

Outcomes

1. Proposed bill to revoke licenses of ISPs supporting pirate websites.
2. Site-blocking collaboration among IPO, NTC and ISPs.

Regulators / Collaborative Parties

1. National Telecommunications Commission (NTC)
2. Optical Media Board
3. Intellectual Property Coalition (IPC)
4. Philippine Association of the Recording Industry (PARI)

Source: The Asia Video Industry Report 2023

against it feels like a Sisyphean task – an unrewarding, fruitless struggle doomed to repetition.

However, Mulready begs to differ, drawing parallels to the global ceaseless war against drug abuse, in which the essence of the battle revolves around harm reduction.

“We’re protecting the creative industry that surrounds the whole distribution network from individuals who are making huge profits from illegal activities.

“I don’t subscribe to the inevitability argument because there is a lot that can be done to minimise the extent of the problem.

“Doing so really requires support from the government and regulators, as the industry cannot do it alone. Otherwise, we’d be fighting in this cat-and-mouse battle with one paw,” he quips.

Dynamic IP blocking

When asked about the most effective anti-piracy strategies, Mulready points to the UK as a model, citing its dedicated intellectual property unit, dynamic IP blocking programme and robust legislation that has set a high standard.

In contrast, the Asia-Pacific region presented a mixed picture. While Singapore, he said, showed promise, the general regional response in curbing digital piracy remains insufficient.

“I wouldn’t like to say one country is better than the other in this region but overall, I think this region really needs to improve its responses to this kind of crime. So, yeah, work to be done here,” says Mulready.

For Malaysia, he believes that there is a need to implement dynamic IP blocking – one of the three site blocking methods – into its anti-piracy arsenal in combating digital pirates.

Dynamic IP blocking differs from the conventional Domain Name System (DNS) and Uniform Resource Locator (URL) blockings, as it stops users from accessing content by blocking specific IP addresses.

If an IP is blacklisted, all content hosted there becomes unreachable, preventing access to sites on that address.

DNS blocking, on the other hand, targets the entire domain, blocking access to all subpages, whereas URL blocking targets specific web pages, blocking individual URLs but not the entire site.

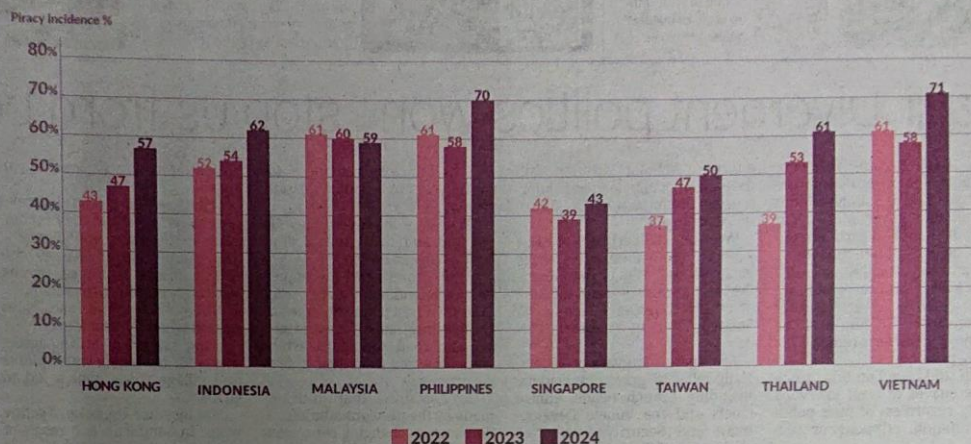
Owing to its speedy and more precise nature, dynamic IP blocking has recently been widely and extensively used worldwide – with excellent implementation seen in the UK and Italy – to combat the digital piracy menace, effectively barring unauthorised streaming and download sites.

What our neighbours are doing

Despite Mulready’s tepid assessment, a concerted effort against digital piracy is underway across South-East Asia.

For example, in Vietnam, its government has announced an ambitious plan to form a specialised unit dedicated to clamping

Incidence of Piracy 2022-2024



Source: Asia Video Industry Association's (AVIA) Coalition Against Piracy, 2024

down on pirate sites.

The unit will see unprecedented coordination between the Vietnamese Ministry of Information and Communications, Ministry of Culture, Ministry of Sports and Tourism and Ministry of Public Security.

Apart from enforcement, the country also recognised the need for affordable and legitimate alternatives, with efforts being taken to reduce barriers for foreign content providers to enter the Vietnamese market.

Meanwhile, the Indonesian government has been equally decisive in its fight against digital piracy.

Stern warnings have been issued without hesitation, even extending to platform providers like Telegram, which was threatened with a nationwide block should it fail to act against illegal online activities that were committed in its ecosystem.

Indonesia has also shown its resolve through legal action. On May 25 last year, the country meted out a significant jail term to a digital pirate, sentencing him to six years in prison for content piracy.

The Philippines is also making bold moves to update its Intellectual Property Code and introduce site-blocking measures.

Its Senate has taken a proactive stance, one supported by major industry players, underscoring a national commitment to safeguarding the livelihood of content creators.

Legislative proposals such as Senate Bill 2150 and Senate Bill 2385 were aimed at restricting access to websites promoting copyright violations and to expand the authority of the country's Intellectual Property Office to initiate site-blocking measures.

Response to cyber threats

In Malaysia, the prosecution of digital piracy cases is often handled through Copyright Law, specifically, Section 43AA which

criminalises the use of streaming technology for copyright infringement.

Nonetheless, like many countries in the region, Malaysia's legislation lacks the comprehensive power to tackle the highly adaptive and borderless nature of digital piracy, allowing online thieves to evade enforcement as long as they operate outside Malaysian soil.

Apart from raiding errant restaurants broadcasting content that was illegally siphoned from legitimate sources, the government has also come up with its own site-blocking initiative, called CyCORE.

CyCORE, however, has two glaring limitations.

Firstly, copyright owners have to manually register their content with CyCORE and secondly, once registered, stringent enforcement of takedowns will only be done for a 14-day period.

Meanwhile, digital pirates have been churning out thousands of piracy links daily.

Despite these efforts, the prevailing attitude towards digital piracy remains largely nonchalant, which is concerning as such criminality is one of the many gateways to cyber threats.

In fact, a study done in Singapore discovered that users of illegal streaming websites and Android TV boxes were up to four times more likely to encounter malware and scams, with half of the ads on illegal sites being high risk.

Nonetheless, when it comes to addressing cybersecurity threats – be it digital piracy, online scams or malware attacks – Malaysia has never been short on the legislative front, having a total of seven laws pertaining to it.

The latest addition was the Cyber Security Act that was passed in Parliament in March – a milestone etched against the worrying backdrop of Malaysia being the eighth most breached country in Q3 2023.

Calling it a good start that

underscored Malaysia's commitment to beefing up its digital defences, cybersecurity expert Murugason R. Thangaratnam, explains that the act has created a baseline to regulate and set industry standards.

“It’s a crucial step forward in strengthening our digital defences, to enhance transparency, accountability and national readiness to address cybersecurity challenges,” says Murugason, who is the chief executive officer of cybersecurity firm, Novem CS.

Nonetheless, Murugason also acknowledges the significant challenges faced by Malaysia and calls for greater accountability, improved communication of efforts and cohesive teamwork, especially at government level.

“Then there is also the general lack of understanding that cybersecurity is not merely a project but rather, a national security,” he remarks.

No silver bullets

Murugason acknowledges that the battle against cyber threats cannot be fought by the public sector alone, reasoning that “there are no silver bullets” for cyber security.

Too many organisations – both public and private – have fallen short in basic cybersecurity measures, he argues, lamenting that the current focus has been too technology-centric and vendor-driven.

“Currently the market in Malaysia does not drive security. If there is no market demand for basic cyber security, then there is little incentive for companies to make security a priority.

“People and processes should always come before technology, and it must be ring-fenced by governance,” says Murugason, stressing that small- and medium-sized enterprises (SMEs) are the most vulnerable towards cyber threats.

As such, he proposes that the government should start devel-

oping incentives and providing resources to help SMEs prioritise cybersecurity, given how said businesses have been the easiest entry point for threat actors.

Reflecting on successful models that Malaysia can emulate, Murugason mentions the US Cybersecurity and Infrastructure Security Agency's Joint Cyber Defense Collaborative (JCDC).

“It’s a powerful example of public-private partnerships,” he says, explaining that JCDC strengthens communication lines between industry and government, and turns collective insights into action.

To share is to empower

While he admits that it was unrealistic to expect the government to stop all cyber-attacks, Murugason nonetheless stresses that there are things in cybersecurity that only the government can do.

Any national strategy for cybersecurity, he explains, should recognise and leverage comparative advantages and avoid duplication of efforts.

“Hence, the need for agencies to work in tandem.

“Cooperation requires a shift in mindset, moving from mere event response to the prioritisation of prevention.

“Building national and industrial resilience is critical,” he says.

Murugason stresses the need for the sharing of information and resources between the public and private sectors, which – if done correctly – can also help cement trust.

“Not all noise is intelligence, and not all intelligence is useful if it is not shared and converted into actionable results.

“Technology is just the enabler, not the solution.

“The challenge with cybersecurity is that it is a battle being fought in a borderless and unrestricted world called the dark web, where laws and treaties mean nothing,” Murugason concludes.

DISEDIKAN
OLEH

NOR SURIANI BINTI MOHD ZIN (S44), BPM
UNIT PERPUSTAKAAN, BPM