Consumer Risk from Piracy in Southeast Asia

Paul A. Watters PhD,
Cyberstronomy Pty Ltd and Macquarie University

Consumer Risk from Piracy in Southeast Asia

Paul A. Watters PhD, Cyberstronomy Pty Ltd and Macquarie University

Executive Summary

Consumers in Southeast Asia who access piracy sites and services are at severe risk of cyber threats from a wide range of criminal actors exploiting unlicensed platforms. Young, affluent, and tech-savvy users in Malaysia, Singapore, Thailand, Vietnam, and Indonesia routinely turn to content - movies, tv shows, live sports, anime and manga - through unlicensed channels such as P2P networks, illicit streams, piracy-enabled set-top boxes, and scam portals.

The aim of this Southeast Asia study is to rigorously quantify and compare the cyber risks facing consumers in the region who engage with various types of piracy services. Building on peer-reviewed methodologies, this research addresses a critical policy question: How much greater is the cybersecurity risk for Southeast Asian consumers using piracy sites compared to mainstream, legitimate platforms?

To quantify the cyber risk posed by these services, this study analyzed the top 30 sites per piracy category in each country, across Streaming, Anime, Streaming Sports, P2P, IPTV, Manga, and Scam sites, using VirusTotal (with over 95 security vendors). Detections were then compared to a control group comprising each country's 30 most popular mainstream sites. A total of 1,200 URLs were empirically analyzed using multi-vendor threat assessment.

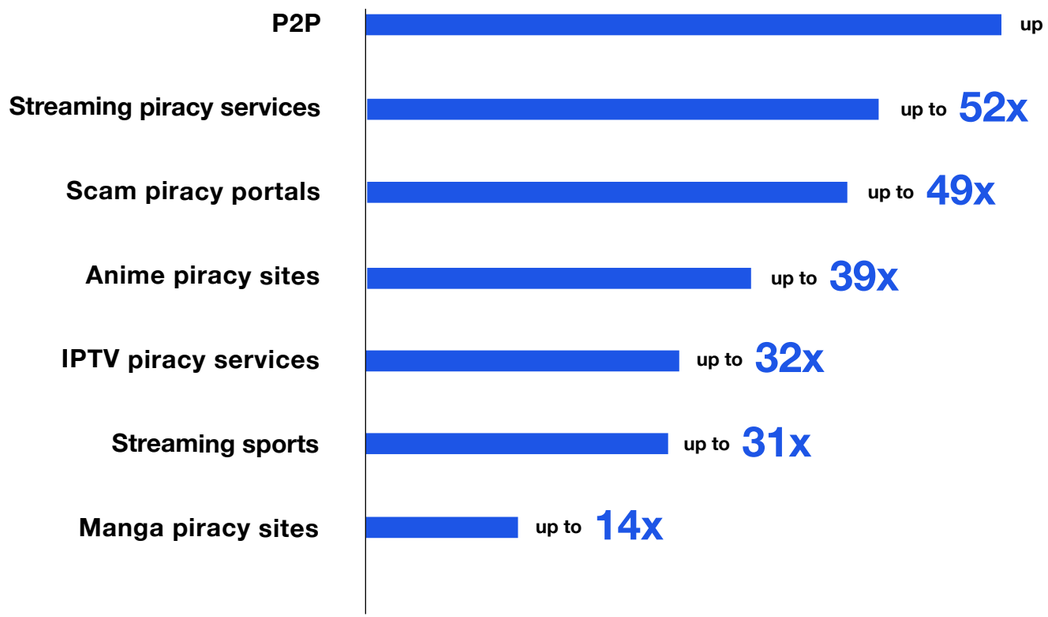
The results are stark. Under both upper bound ("best-case") and lower bound ("worst-case") counting assumptions, piracy sites generated vastly more threat detections than legitimate sites. On average, piracy platforms presented 19.65 threat detections (best-case; mean Relative Risk ≈ 22.40×) and 26.55 detections (worst-case; mean RR ≈ 27.91×), with P2P, scam, and streaming services identified as the riskiest categories.

In conclusion, this study offers granular, cross-country insights designed to inform evidence-based policy, regulatory reform, law enforcement resource allocation, and consumer education.

Key Findings

Relative Risk of Encountering a Cyber Threat by Piracy Type

(Worst-Case, Southeast Asia)
(All figures are 'up to x higher risk' compared to mainstream sites)



- **Relative Risk by Service Type**
  - » **P2P networks:** up to **65× higher** risk than legitimate sites
  - » **Streaming piracy services**: up to **52x higher** risk
  - » **Scam piracy portals**: up to **49× higher** risk
  - » **Anime piracy sites**: up to **39× higher** risk
  - » **IPTV piracy services**: up to **32× higher** risk
  - » **Streaming sports**: up to **31× higher** risk
  - » **Manga piracy sites**: up to **14× higher** risk
- **Overall Risk × 22.40:** In the best-case, consumers face on average more than a 22-fold increase in cyber-threat detections on piracy sites versus mainstream control sites.
- **Top-Risk Categories:** In the worst-case, P2P networks (average 53.20 detections), scam portals (average 44.80 detections), and general streaming feeds (35.60 detections) carry the highest relative risks.
- **Market Details:** Indonesia, Singapore, and Malaysia have the highest average relative risks - each approaching or exceeding a 34-fold increase over legitimate sites; notably, control sites in Singapore, Malaysia, Indonesia, and Thailand had virtually zero detections, underscoring the effectiveness of mainstream platforms' cybersecurity.
- **Put simply:** There are almost no cyber risks on the most popular mainstream websites, but all piracy services show hugely elevated cyber risk.
- **Cross-Country Consistency:** Every piracy service category demonstrated elevated threats in all five countries, with P2P, scam, and streaming sites being the most consistently risky.
- **Regional Pattern**: While legitimate sites are generally very safe, consumers using piracy services anywhere in Southeast Asia are exposed to dramatically higher and preventable cyber risks, regardless of country.
- **Policy Implications:** These findings provide a robust evidence base for targeted policy reform, law enforcement resource allocation, and urgent consumer education. Given the stark disparity between mainstream and piracy platforms - especially in high-risk countries such as Malaysia, Singapore, and Indonesia - coordinated action is strongly recommended to protect consumers from malware, phishing, and other cyber threats linked to digital piracy.

Contents

01

Introduction

What is digital piracy?

Introduction

This study examines the consumer impact of digital piracy across Southeast Asia[1] in the context of cybersecurity risk. The study uses threat data associated with a range of piracy services, across five major economies in the region, to pave the way for targeted mitigation measures - such as regulatory reform, strengthened law-enforcement capabilities, and consumer-focused education. Using an empirical approach, the research rigorously addresses the central question: How risky are piracy sites for consumers in Southeast Asia[2]?

WHAT IS DIGITAL PIRACY?

Digital piracy is the unauthorized acquisition, reproduction or distribution of copyrighted content - in this case across Southeast Asia - without permission or payment to rightsholders. It encompasses everything from downloading bootleg movies and music to accessing live sports streams or fan-subbed anime without a license.

Some of the most common piracy service models in Southeast Asia include:

- **Illicit Streaming**[3] involves accessing content in real-time over the internet without downloading the entire file. Illicit streaming services provide unauthorized access to movies, TV shows, music, and more, often through subscription-based models or free platforms supported by ads.
- **Streaming Sports piracy**[4] sites provide live feeds of sporting events - football, basketball, esports - ripped from pay-TV or official broadcast streams and rebroadcast unofficially.
- **P2P (P2P) networks**[5] are systems where users can share files directly with each other. P2P networks are a decentralized way of sharing files, allowing individuals to upload and download unlicensed content directly from other users' computers
- **Scam**[6] piracy sites are fraudulent websites that deceive users into believing they are accessing legal content or services. These sites might offer pirated content under the guise of legitimacy, tricking users into paying for access or downloading malicious software. They often contain no illicit content.
- **IPTV Piracy Subscription Services**[7] are piracy services that require a subscription fee and offer content which would include live channels of film/TV and sports content. These services may also include some VOD (video on demand) as well. Typically, consumers pay a single subscription fee to access multiple paid services, however, the revenue is not paid to rightsholders.
- **Anime**[8] piracy sites are popular portals that stream or offer downloads of Japanese animation (TV series, films, OVAs) without any license or permission from rightsholders. These sites typically aggregate unauthorized video files or embedded streams.
- **Manga**[9] piracy sites are digital repositories that provide access to complete chapters or volumes of manga without official distribution rights. These sites scrape or host scanned/computer-generated translations and make them available for in-browser reading or bulk download without paying any license fees.

Each of these services operates with distinct technical implementations (stream ripping, P2P torrent swarms, ad-injection, credential phishing) and business incentives (ad revenue, subscription takings, data theft). Together, they form an interlinked piracy–cybercrime ecosystem[10]. Serious consumer harms - from malware infections to financial fraud - can flow from this diversity of unlicensed services.

02

Social and Economic Consequences of Piracy

Social and Economic Consequences of Piracy

Digital piracy in Southeast Asia extends far beyond lost revenues, reshaping cultural norms, creative ecosystems and regional economies[11]. Economic growth and innovation rely on an enforceable intellectual property protection system, while the rise of piracy poses challenges to socioeconomic stability, with prevention[12] being a key strategy recommended to policymakers. A peer-reviewed survey of 400 university students across China, Vietnam, South Korea, and Japan found that 51% of respondents reported engaging in peer-to-peer (P2P) music piracy at least once in the previous year[13]. Prevalence was highest in China and South Korea, significantly exceeding that in Japan, while Vietnam showed somewhat lower rates. Notably, the study found that social and cultural norms - rather than differences in legal frameworks, copyright tradition, or economic factors - were the most powerful predictors of piracy behavior. Female students were generally less likely to participate in piracy, though this effect disappeared when controlling for country. Overall, the findings suggest that local social attitudes play a decisive role in shaping digital piracy patterns across Asian countries, and that uniform legal reforms alone are unlikely to reduce infringement without addressing these underlying norms.

A recent study explored motivations underlying digital piracy – the authors identified key drivers such as the refusal to pay for content, the proliferation of subscription services, and the profitability of illegal activities. They emphasize that social consensus - where piracy is normalized within a community - significantly influences individuals' intentions to engage in piracy. This effect is further moderated by individuals' tendencies to conform and their situational ethics. The study concludes that addressing digital piracy effectively requires understanding these underlying social and ethical dynamics, suggesting that interventions should focus on altering social norms and ethical perceptions rather than solely relying on legal deterrents[14].

SOCIAL CONSEQUENCES

Digital piracy poses a long-term threat to Southeast Asia's cultural preservation and dissemination. The widespread availability of unauthorized content undermines the value of local creative works, discouraging investment and diminishing the perceived worth of cultural products. Reduced demand for legitimate local content weakens incentives for authentic cultural production, threatening the transmission of cultural heritage.

Locally produced content often reflects the language, customs, beliefs, and social norms unique to a community or nation. By portraying local stories, histories, and ways of life, such content helps new generations learn about, understand, and internalize cultural values. Piracy reduces the business case for further investment in local industry – according to AVIA, in Malaysia, the annual losses are RM3 billion[15].

Surveys indicate a normalization of piracy, especially among younger, digitally native populations[16]. This shift in perception weakens respect for intellectual property rights and reduces the stigma associated with infringement. As a result, creators and cultural industries face declining revenues and limited resources to develop or promote authentic cultural products, further endangering local heritage and diversity.

Finally, in a study of attitudes towards piracy in Vietnam, Nguyen and Tran[17] found that moral obligation was identified as a significant negative predictor of the intention to commit digital piracy. Individuals with a strong sense of moral responsibility are less likely to engage in piracy, highlighting the importance of ethical considerations in curbing such behavior. Thus, when piracy among local, young people risks becoming entrenched, it reflects not only an erosion of moral norms but also signals broader social harm, as the normalization of piracy can undermine respect for intellectual property, diminish trust in creative industries, and weaken the foundations of lawful digital citizenship within these communities.

ECONOMIC CONSEQUENCES

Digital piracy significantly undermines the economic foundations of Southeast Asia's creative industries. When consumers turn to pirated films, music, software, or digital media, legitimate creators and businesses lose vital income streams. This loss in revenue translates directly into fewer opportunities for local artists, writers, technicians, developers, and production staff—resulting in job losses and discouraging young talent from entering creative professions.

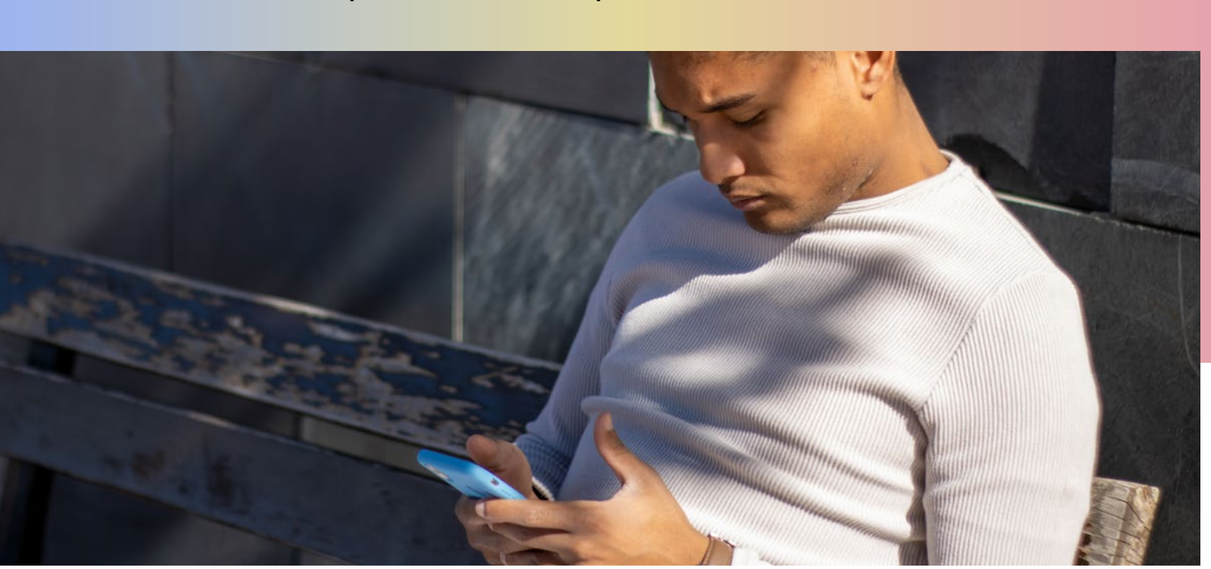
To illustrate just how serious the financial impact is, Lumbanraja et al., 2018[18] undertook a study of economic losses due to film piracy in Indonesia. Within four cities, losses in 2017 were estimated to be IDR1.5 trillion; extrapolating to the whole of Indonesia (at the time), national losses might be as high as USD1.72 billion.

In addition to the direct losses, reduced sales mean less profit for legitimate businesses, leading to lower corporate tax contributions and sales/consumption tax collections. Because piracy networks typically operate outside the formal economy and rarely pay taxes, governments face shrinking public revenues. This limits resources available for essential public services such as schools, hospitals, infrastructure, and cultural development programs.

Furthermore, the lack of financial return makes local content production riskier and less attractive to investors, stifling innovation and reducing the diversity of stories and perspectives available in the region. Legitimate digital services also struggle to compete with the artificially low prices offered by pirate operations, putting additional pressure on honest businesses and slowing the growth of the region's digital economy.

CONSUMER RISKS

When consumers enter payment details on a piracy site - whether to unlock "premium" streams or pay a nominal subscription fee - they expose their cards to criminal misuse. A Digital Citizens Alliance (DCA) study[19] found that roughly one in ten credit-card transactions on piracy platforms resulted in unauthorized charges within 30 days, as fraudsters harvest card data and either resell it on the dark web or exploit it for high-value purchases. Victims often don't discover the fraud until statements arrive, forcing them to dispute charges, endure temporary holds on their accounts and face potential credit-score impacts.



Illicit content portals frequently masquerade as legitimate services - using cloned brand logos or copycat domains - to trick consumers into thinking they're engaging with recognized platforms. When these schemes collapse (for instance, by vanishing overnight), victims lose access to any promised service and risk exposure of their personal data (names, email addresses, phone numbers) to affiliates who may spam, harass or sell that information. Beyond the immediate financial loss, this "bait-and-switch" undermines trust, making consumers wary of both illicit and genuine digital offerings.

Based on previous research, however, the most significant consumer risks are associated with cybersecurity[20]. These are summarized below.

Malware & Drive-by Downloads

Piracy sites often bundle trojans, worms or keyloggers in seemingly innocuous downloads or embedded players. Simply visiting a compromised streaming portal can trigger a "drive-by" download that installs malicious code without user consent, leading to system slowdowns, corrupted files or covert backdoor access for attackers.

Ransomware & Cryptojacking

Many illicit download hubs and P2P networks carry ransomware payloads that encrypt your data and demand payment for its release. Others secretly run cryptomining scripts in your browser or on your device (cryptojacking), consuming CPU/GPU resources and degrading hardware performance without any visible indication.

Phishing & Credential Theft

Piracy platforms often imitate legitimate login or payment pages to harvest usernames, passwords and two-factor tokens. These stolen credentials can be reused on banking or social-media accounts, enabling identity theft, unauthorized fund transfers and account takeovers.

Spyware & Data Exfiltration

Hidden spyware and keyloggers in cracked software or APKs monitor keystrokes, take periodic screenshots and exfiltrate personal documents to remote servers. Victims may never know their confidential emails, photos or financial records have been silently copied and trafficked to cyber-criminal marketplaces.

Botnet Recruitment & Network Compromise

By installing P2P clients or cracked network-tools, users can unwittingly join botnets that coordinate distributed denial-of-service (DDoS) attacks, spam campaigns or additional malware distribution. This not only endangers the infected device but can also degrade home or office networks and expose other systems on the same LAN.

Together, these cyber risks illustrate that engaging with pirated content not only violates copyright but also opens a direct path for serious security breaches, financial loss and privacy invasion. Organized-crime syndicates have embraced digital piracy as a low-risk, high-reward venture[21]: by running or financing illicit streaming portals, P2P hubs and counterfeit software marketplaces, they monetize copyrighted content through ad-fraud[22], subscription scams and direct sales[23], leveraging their established counterfeit-goods networks to reach global audiences at scale.

These piracy platforms also serve as ideal conduits for money laundering - illicit revenues from ads and paywalls can be cycled through shell companies or cryptocurrency mixers to obscure trails - and as launchpads for wider cyber-crime. Syndicates routinely partner with hackers to embed malware, conduct phishing campaigns and harvest user data, all while operating across jurisdictions[24] and exploiting legal gaps, making comprehensive enforcement and domain-takedown efforts exceptionally difficult.

A CYBER THREAT MODEL FOR DIGITAL PIRACY

A cyber threat model is a structured framework for identifying, categorizing and prioritizing the ways an adversary might compromise a system or service. It maps out valuable assets, potential vulnerabilities, attacker goals and likely attack vectors, enabling defenders to focus resources on the highest-risk scenarios. In the context of Southeast Asian piracy ecosystems, threat modeling reveals how malicious actors leverage unlicensed Streaming, Anime, Sports, P2P, IPTV, Manga and Scam sites to deliver malware, harvest credentials and pivot into broader network intrusions.

1. **Site Operators**
   These are the individuals or groups who build and maintain piracy platforms - whether web-streaming portals, IPTV services or torrent trackers. Because they control the infrastructure, site operators can inject drive-by exploits into embedded players, bundle malware in client-side applications (e.g. Android TV box apps) and integrate malicious ad or update channels. Their position grants the broadest reach: every visitor or subscriber is potentially exposed to hidden payloads that silently install backdoors, cryptominers or spyware.
2. **Uploaders**
   On P2P, Anime and Manga sites, community contributors (“uploaders”) seed or host specific files. Actors in this role may embed malware within seemingly benign downloads - such as subtitle files, ZIP/RAR archives or “cracked” media players - knowing that users will unpack and run these components locally. Because end users expect only media content, these injections often evade immediate detection, allowing malware and ransomware to propagate rapidly through P2P swarms.
3. **Third-Party Injectors**
   Beyond operators and uploaders, external injectors exploit shared ad networks, common web frameworks and known vulnerabilities in site code. They deliver malvertisements or perform cross-site scripting (XSS) attacks that slip malicious JavaScript into pages, capturing cookies or redirecting users to phishing and exploit kits. Often stealthy and independent of the platform’s owners, these actors amplify risk by turning even otherwise benign piracy sites into vectors for drive-by downloads and credential theft.
4. **Site Hackers**
   Beyond the roles of operators, uploaders and third-party injectors, a fourth actor class - **site hackers** - targets the piracy platforms themselves, breaching their infrastructure to insert or amplify malicious content. They are often criminal groups or “script kiddies” seeking easy pickings, since many pirate portals run outdated CMSs or neglect server hardening. Motivations range from financial (ransomware or data theft) to strategic (using the compromised site as a springboard into other networks). Their typical methods include exploiting unpatched vulnerabilities in web frameworks, plugins or management panels (e.g. SQL injection, remote code execution), credential stuffing or phishing site admins to harvest login details and gain administrator privileges, and privilege escalation on poorly configured Linux/Windows hosts to install rootkits or backdoors. The impact on end users and broader networks includes server-side malware injection, ensuring every visitor - even to innocuous pages - receives exploit kits, cryptominers or spyware, and potentially pivoting into adjacent networks, as compromised hosting environments often share infrastructure with legitimate services (e.g. DNS providers, CDN nodes), multiplying the blast radius of an attack.

The model is summarized in Figure 1.

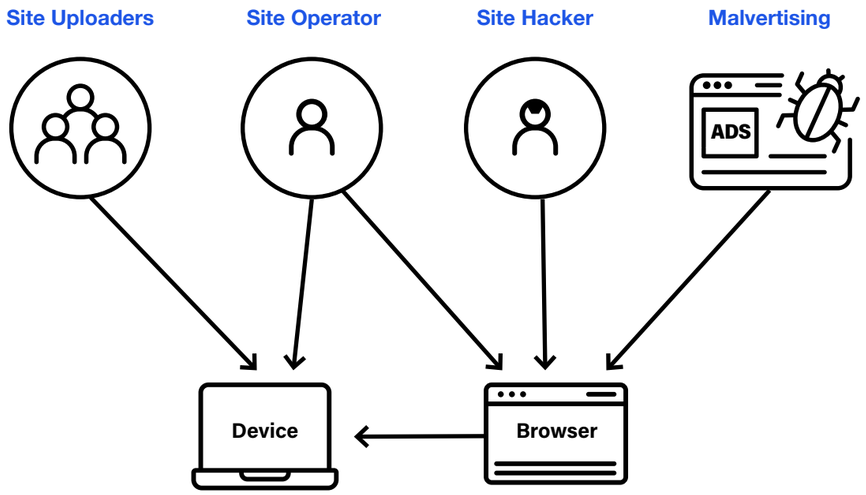


Figure 1 – Traditional Piracy Threat Model

In recent years, piracy in Southeast Asia has partially migrated from P2P swarms and ad-filled web portals to purpose-built Illicit Streaming Devices (ISDs) - low-cost set-top boxes or “smart” dongles pre-loaded with unlicensed add-ons. Unlike traditional piracy, which relied on user-installed software or social communities rewarding uploaders, ISDs offer “piracy-as-a-service”: consumers simply plug in the device, pay a flat fee, and stream live TV, movies or niche content through a familiar, legally-styled interface. Because no technical skills or torrent clients are needed, ISDs have dramatically lowered the barrier to entry and driven explosive uptake across Singapore, Malaysia, Thailand, Vietnam and Indonesia.

But that convenience comes with a fundamentally different threat model (see Figure 2 – Threat Model – ISDs). By embedding themselves on the local network - often with root access to home routers or LAN segments - ISDs create an attacker foothold that can pivot laterally to laptops, NAS drives or even children’s learning tablets. A compromised box can silently receive firmware updates carrying remote-access trojans or cryptomining scripts, bypassing firewall protections under the guise of legitimate entertainment. History offers a warning: Mirai’s 2016 campaign co-opted insecure IoT devices into a global botnet[25], and similarly weaponized ISDs could be marshalled - perhaps even by a nation-state actor - into large-scale DDoS, espionage or ransomware campaigns. This “maskirovka” approach - hiding malicious deployments within expected software updates - turns what looks like an innocuous streaming box into a potent vector for cyber-crime and network intrusion.

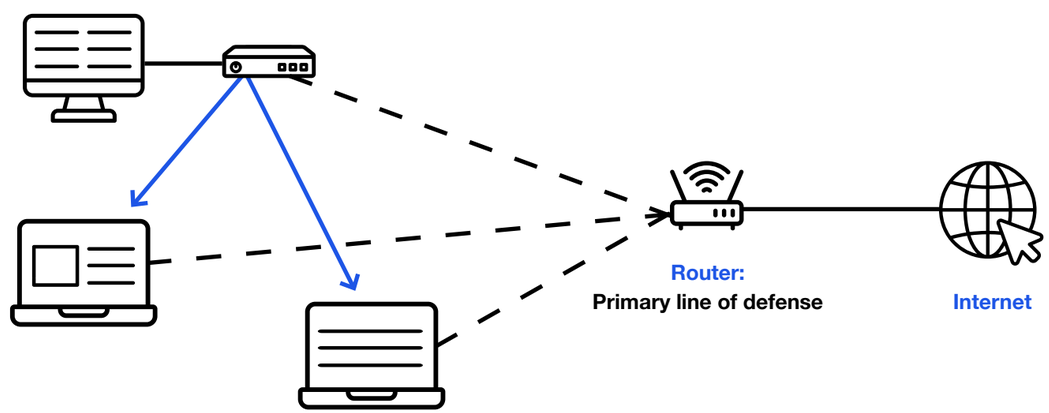


Figure 2 – Threat Model – Undermining Bastion Defenses

CYBERCRIME AND CONSUMER WEALTH IN SOUTHEAST ASIA

Consumers' economic circumstances across Singapore, Malaysia, Thailand, Vietnam and Indonesia vary widely, but according to McKinsey[26], can be characterized by significant year-on-year GDP growth. In Singapore, very high GDP per capita and robust social transfers translate into strong purchasing power, high savings rates and broad access to credit. Malaysia and Thailand sit in the upper-middle income bracket, with sizeable middle classes but rising household debt - particularly mortgages and auto loans - that can strain monthly budgets. In Vietnam and Indonesia, rapid economic growth has lifted millions into the middle class, yet average incomes remain lower and social safety nets are less comprehensive, leaving more families vulnerable to unexpected expenses. Across all five markets, expanding financial-education programs and growing fintech adoption have improved literacy and inclusion, but disparities persist between urban and rural, formal and informal sectors[27].

Why are Southeast Asian consumers attractive targets for cyber threats?

As wealth grows in Southeast Asia, consumers will increasingly become targets for cybercriminals. Some factors that contribute to this targeting include:

- **High Internet & Mobile Penetration**
  With smartphone ownership exceeding 75% in each of these countries and aggressive rollout of 4G/5G networks, consumers maintain a constant online presence - providing attackers with abundant entry points via banking apps, e-wallets and social platforms.

- **Rapid Digital Finance Adoption**
  The shift toward mobile payments, QR-based transfers and app-based lending (especially in Singapore and Malaysia) creates lucrative opportunities for phishing, credential-stealing malware and spoofed payment pages.

- **Growing Disposable Incomes**
  Rising wages and expanding middle classes - most notably in Vietnam and Indonesia - make residents attractive for financial fraud, ranging from staged "tech support" scams to premium-rate SMS traps.

- **Variable Cybersecurity Awareness & Regulation**
  While Singapore boasts stringent data-protection laws and public campaigns, awareness and enforcement may be less strict in parts of Malaysia, Thailand, Vietnam and Indonesia. Cybercriminals exploit these gaps with localized phishing in Malay, Thai, Vietnamese or Bahasa-Indonesia, increasing success rates.

- **Prevalence of Pirated Services**
  High use of unlicensed streaming, ISD boxes and P2P networks not only exposes devices to malware but also normalizes risk-taking behavior - blurring the line between casual downloading and more dangerous cyber-crime vectors.

PROTECTIVE FACTORS IN SOUTHEAST ASIA'S CYBER POLICY AND REGULATORY RESPONSES

Across Singapore, Malaysia, Thailand, Vietnam and Indonesia, governments have introduced comprehensive national cybersecurity strategies that set clear priorities - ranging from critical-infrastructure protection to threat intelligence sharing - and mandate cross-sector collaboration. Singapore's Cybersecurity Strategy and the Cybersecurity Act create a governance framework for licensing and auditing essential service providers, while Malaysia's National Cybersecurity Policy, Thailand's National Cybersecurity Strategy, Vietnam's Law on Cybersecurity and Indonesia's PP 71/2019 on the Government's Use of the Internet each enshrine proactive risk-management requirements and minimum technical standards for both public and private entities.

Robust legal and regulatory frameworks underpin those strategies. Each country has updated its cybercrime legislation to criminalize unauthorized access, malware distribution and online fraud: Malaysia's Computer Crimes Act, Thailand's Computer Crime Act, Vietnam's penal code amendments and Indonesia's ITE Law (with stricter breach-reporting obligations under PP 82/2012). Data-protection regimes - Singapore's PDPA, Malaysia's PDPA, Thailand's PDPA, Vietnam's draft data-protection law and Indonesia's PDP Law - impose safeguards on how personal information is collected, stored and shared, creating deterrence against mass data harvesting by illicit services.

Institutional collaboration - both public-private and inter-agency - is a cornerstone of regional resilience. National CERTs (SG-CERT, MyCERT, ThaiCERT, VNCERT and ID-CERT) operate 24×7 monitoring, incident-response and community-alert functions, while public-private partnerships such as Singapore's Cybersecurity Consortium, Malaysia's CyberSecurity Malaysia collaborations and Thailand's Cyber Threat Intelligence Sharing Platform foster real-time exchange of threat indicators. Regulators also work with telecom operators and major platforms to block known malicious domains and sinkhole botnets used by piracy-related malware.

Finally, education, workforce development and international cooperation amplify those domestic efforts. Governments fund cyber-hygiene campaigns in schools and SMEs (e.g. Malaysia's CyberSAFE, Singapore's Cyber Youth Program, Thailand's Cybersecurity Talent Development), and invest in national cyber-ranges to upskill responders. At the regional level, ASEAN's Cybersecurity Cooperation Strategy (ACCS), the ASEAN-CERT Network and partnerships with APEC, ASEANAPOL and Interpol help harmonize best practices and coordinate cross-border takedowns of illicit streaming and piracy infrastructures. These layered policies, regulations and cooperative mechanisms collectively raise the bar on defensive readiness and reduce consumers' exposure to cybercrime vectors.

However, there is very little dedicated activity by governments to address cybersecurity risks specifically arising from the digital piracy ecosystem. Previous studies in the region have indicated a high level of cyber risk for consumers. In this study, a direct comparison is planned to understand the relative cyber risks faced by consumers who use a broad range of piracy services, across five nations within the region.

03

Methods

Methods

Data were collected from five Southeast Asian countries for the purposes of this study – Malaysia, Indonesia, Thailand, Vietnam and Singapore. The method used to assess cyber risk for each country on piracy websites relied on VirusTotal, a Google tool that scans websites for malware, phishing, suspicious, malicious, or spam content. VirusTotal checks against a database from over 95 antivirus vendors and runs potentially harmful code in a secure environment to determine threats. This tool is widely recognized for antivirus research worldwide. The collected data from VirusTotal helped create risk metrics, like the likelihood of encountering threats, comparing them to safe mainstream sites.

The Alliance for Creativity and Entertainment (ACE), a leading anti-piracy association, provided a list of piracy websites offering unauthorized film and TV content, along with fraudulent sites popular in the five countries[28]. ACE compiled this list based on copyright removal requests, site blocks in various countries, and other reliable sources. From this list, specific samples were chosen for comparison. Additionally, a control sample from each country's top 30 most popular mainstream websites was assessed for a valid comparison between piracy sites and typical websites. Each sample comprised 30 sites, allowing for reliable population inferences using sample standard deviation to calculate standard error. This method ensured representative samples and an experimental design with a control for valid conclusions. Where a piracy site was also present in the control sample, the next most popular site in the top sites list for that country was substituted. Sites associated with illicit activity - such as unregulated online gambling, pornography, cyberlockers and similar illicit services - were excluded from the control list to avoid conflating their distinct threat profiles with piracy-related risks. URLs linked to advertising networks were also excluded.

We gathered samples for specific categories based on consumers' site visits in May 2025, for each country:

- **The top 30 Streaming sites**
- **The top 30 Anime sites**
- **The top 30 Streaming Sports sites**
- **The top 30 P2P sites**
- **The top 30 IPTV sites**
- **The top 30 Manga sites**
- **The top 30 Scam sites**

During the sampling period, the "Top 30" represented the most visited sites, aligning with the Pareto Principle, indicating that a small number of sites likely attracted the most traffic. The "scam" piracy sites, as verified independently by ACE, did not host actual pirated content.

Drawing a distinction between piracy and "scam" piracy sites was deemed to be important. "Scam" piracy sites don't host any content; instead, they deceive users into purchasing overpriced subscriptions after obtaining their credit card details. While all piracy sites pose risks, it was anticipated that "scam" sites could be even riskier due to their overtly deceptive nature.

04

Results

Worst-Case and Best-Case Likelihood Scenarios

Results

The URLs for the 1,200 websites in the sample across all seven categories (Streaming piracy, Anime piracy, Streaming Sports piracy, P2P, IPTV piracy, Manga piracy, Scam and Control) and across five countries were uploaded to VirusTotal, and the results tabulated across six cyber risk categories (malicious, malware, suspicious, phishing, spam and not recommended). These categories can be defined as follows[29]:

- **Malicious – human confirmation that a site contains cyber threats**
- **Suspicious – machine detection that a site contains cyber threats**
- **Malware – malware distributed from the site**
- **Phishing – site used to steal users' credentials**
- **Spam – site used for unsolicited email, popups and automatic commenting**
- **Not Recommended – potentially unwanted software distribution**

These categorizations are based on reports from more than 95 partners comprising the world's largest cybersecurity threat detection companies and represent a community-based effort to identify sites that are actively engaged in delivering cyber threats[30]. For each detection company, only one category per site is reported, based on their assessment of the risks on the site.

WORST-CASE AND BEST-CASE LIKELIHOOD SCENARIOS

In each analysis, we provide a worst-case and best-case likelihood estimate[31]. This is because multiple reports in each threat category are independently reported by the antivirus vendors on VirusTotal. Since each security vendor uses their own definitions, and maintains their own proprietary threat database, the best-case estimate is very conservative, and assumes all detections from each vendor is identifying the same malware sample. The worst-case estimate then assumes that all vendors are identifying completely independent samples. By looking at the threat reports for each cyber threat, most detections are different, however, in the interests of transparency, a range indicating different levels of confidence is provided.

Tables 1 and 2 show the worst-case and best-case results for the number of detected cyber threats per category and per country, with the raw distributions shown in Figures 3 and 4. In the worst-case, the overall average number of detections was 26.55, with Indonesia, Malaysia and Singapore both receiving the highest number (average 30.00-30.38 detections each). In the best-case, the average number of detections was 19.65, with Singapore and Indonesia encountering an average 21.75-22.00 detections each. For both the best-case and the worst-case, the riskiest categories were P2P, Scam and Streaming piracy sites respectively.

Tables 3 and 4 average likelihood of encountering a cyber threat. In simple terms, where the likelihood is greater than one, consumers are – on average – likely to encounter one cyber threat. Thus, when reading the table, given that 30 sites were analyzed in each country and across each category, any value greater than 30 implies that – on average – a consumer will encounter at least one cyber threat. These examples are colored blue for easy reference.

Finally, the relative risk of encountering a cyber threat is calculated. By using a control set of mainstream websites, we can calculate just how elevated this risk is compared to normal browsing of the most popular mainstream websites. Tables 5 and 6 show the relative risk calculation, that takes the average detections data, and divides by the detections value of the control group, for the worst- and best-case likelihood estimates respectively.

The relative risk for consumers is extraordinarily high, in most cases, compared to the control condition. For P2P, the risk is 65X higher in Indonesia, 62× higher in Singapore, in the worst-case, with 27.91× average higher risk overall. The overall average RR was 22.40× for the best-case, all countries and categories. The results are shown in Figures 5 and 6. Singapore had the highest overall RR at 25.14×, followed by Indonesia at 24.71×, and Malaysia at 23.71× in the best-case.

The results indicate that different jurisdictions within the region have different risk outcomes, potentially based on some of the key factors described in the Introduction, including policy, regulation and resourcing for law enforcement. These outcomes will be discussed further in the Discussion section. One issue to note is the complete absence of cyber threats on the Top 30 control sites for Malaysia, Singapore, Indonesia and Thailand. This likely reflects the increased policy and operational focus on cybersecurity among global corporations and governments within the region. For RR calculation purposes, detections were nominally set to 1, to avoid division by zero. Setting zero counts to one is effectively a form of continuity correction (or “pseudo-count”) commonly used in epidemiology and contingency-table analysis to avoid infinite or undefined Relative Risk estimates when a cell is zero. By adding a small

	Malaysia	Singapore	Thailand	Vietnam	Indonesia	Average
Streaming	52.00	38.00	21.00	33.00	34.00	35.60
Anime	25.00	34.00	20.00	10.00	39.00	25.60
Streaming Sports	31.00	24.00	11.00	12.00	16.00	18.80
P2P	49.00	62.00	46.00	44.00	65.00	53.20
IPTV	22.00	32.00	21.00	12.00	29.00	23.20
Manga	14.00	14.00	5.00	8.00	12.00	10.60
Scam	47.00	36.00	49.00	45.00	47.00	44.80
Control	0.00	0.00	0.00	2.00	1.00	0.60
Average	30.00	30.00	21.63	20.75	30.38	26.55

Table 1 – Cyber Threat Detections by Piracy Service Type (Worst-Case)

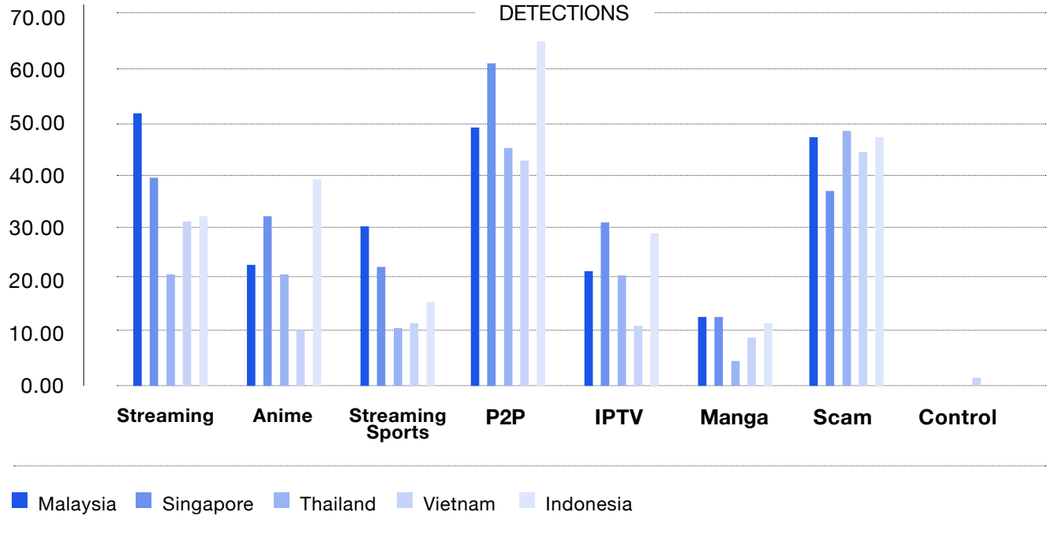


Figure 3 – Cyber Threat Detections by Piracy Service Type (Worst-Case)

	Malaysia	Singapore	Thailand	Vietnam	Indonesia	Average
Streaming	30.00	31.00	20.00	28.00	29.00	27.60
Anime	20.00	27.00	14.00	9.00	26.00	19.20
Streaming Sports	18.00	16.00	9.00	9.00	12.00	12.80
P2P	42.00	48.00	42.00	39.00	51.00	44.40
IPTV	11.00	13.00	10.00	10.00	13.00	11.40
Manga	11.00	12.00	5.00	8.00	10.00	9.20
Scam	34.00	29.00	31.00	35.00	32.00	32.20
Control	0.00	0.00	0.00	1.00	1.00	0.40
Average	20.75	22.00	16.38	17.38	21.75	19.65

Table 2 – Cyber Threat Detections by Piracy Service Type (Best-Case)

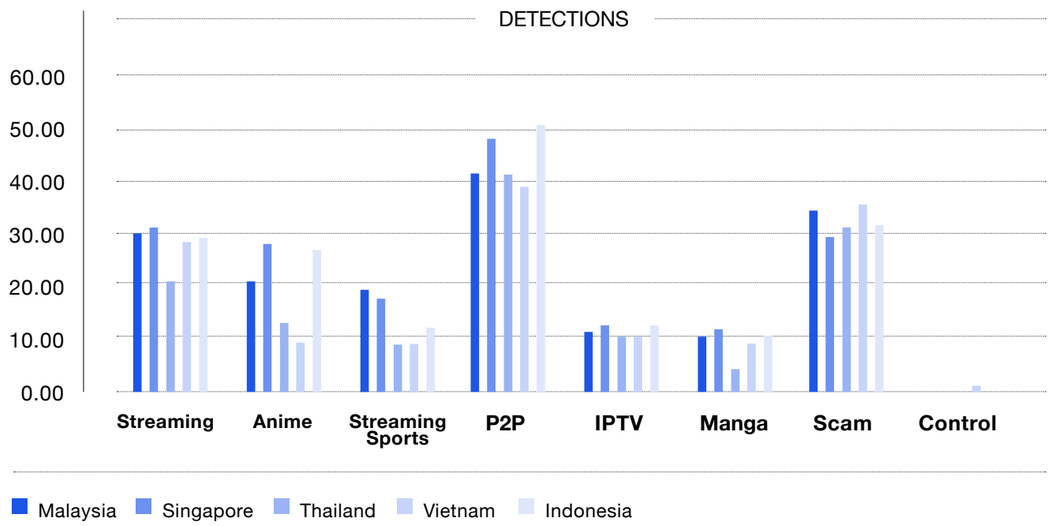


Figure 4 – Cyber Threat Detections by Piracy Service Type (Best-Case)

	Malaysia	Singapore	Thailand	Vietnam	Indonesia	Average
Streaming	1.73	1.27	0.70	1.10	1.13	1.19
Anime	0.83	1.13	0.67	0.33	1.30	0.85
Streaming Sports	1.03	0.80	0.37	0.40	0.53	0.63
P2P	1.63	2.07	1.53	1.47	2.17	1.77
IPTV	0.73	1.07	0.70	0.40	0.97	0.77
Manga	0.47	0.47	0.17	0.27	0.40	0.35
Scam	1.57	1.20	1.63	1.50	1.57	1.49
Control	0.00	0.00	0.00	0.07	0.00	0.01
Average	1.00	1.00	0.72	0.69	1.01	0.88

Table 3 – Average Likelihood of Encountering a Cyber Threat by Piracy Type (Worst-Case)

	Malaysia	Singapore	Thailand	Vietnam	Indonesia	Average
Streaming	1.00	1.03	0.67	0.93	0.97	0.92
Anime	0.67	0.90	0.47	0.30	0.87	0.64
Streaming Sports	0.60	0.53	0.30	0.30	0.40	0.43
P2P	1.40	1.60	1.40	1.30	1.70	1.48
IPTV	0.37	0.43	0.33	0.33	0.43	0.38
Manga	0.37	0.40	0.17	0.27	0.33	0.31
Scam	1.13	0.97	1.03	1.17	1.07	1.07
Control	0.00	0.00	0.00	0.03	0.00	0.01
Average	0.69	0.73	0.55	0.58	0.72	0.65

Table 4 – Average Likelihood of Encountering a Cyber Threat by Piracy Type (Best-Case)

	Malaysia	Singapore	Thailand	Vietnam	Indonesia	Average
Streaming	52.00	38.00	21.00	16.50	34.00	32.30
Anime	25.00	34.00	20.00	5.00	39.00	24.60
Streaming Sports	31.00	24.00	11.00	6.00	16.00	17.60
P2P	49.00	62.00	46.00	22.00	65.00	48.80
IPTV	22.00	32.00	21.00	6.00	29.00	22.00
Manga	14.00	14.00	5.00	4.00	12.00	9.80
Scam	47.00	36.00	49.00	22.50	47.00	40.30
Average	34.29	34.29	24.71	11.71	34.57	27.91
Average (Excluding Manga)	37.67	37.67	28.00	13.00	38.33	30.93

Table 5 – Relative Risk of Encountering a Cyber Threat by Piracy Type (Worst-Case)

	Malaysia	Singapore	Thailand	Vietnam	Indonesia	Average
Streaming	30.00	31.00	20.00	28.00	29.00	27.60
Anime	20.00	27.00	14.00	9.00	26.00	19.20
Streaming Sports	18.00	16.00	9.00	9.00	12.00	12.80
P2P	42.00	48.00	42.00	39.00	51.00	44.40
IPTV	11.00	13.00	10.00	10.00	13.00	11.40
Manga	11.00	12.00	5.00	8.00	10.00	9.20
Scam	34.00	29.00	31.00	35.00	32.00	32.20
Average	23.71	25.14	18.71	19.71	24.71	22.40
Average (Excluding Manga)	25.83	27.33	21.00	21.67	27.17	24.60

Table 6 – Relative Risk of Encountering a Cyber Threat by Piracy Type (Best-Case)

Focusing specifically on audiovisual piracy (i.e., excluding Manga), also shown in Table 5 and 6, we can see that the averages rise in each category. The data show that audiovisual piracy modalities (streaming, anime, sports, P2P, IPTV, scam sites) are consistently associated with significantly higher risks of encountering cyber threats compared to Manga piracy. In both best-case and worst-case scenarios, removing Manga from the calculation raises the average risk scores for every country, highlighting that Manga sites pose lower cyber risks than sites or services offering audiovisual content.

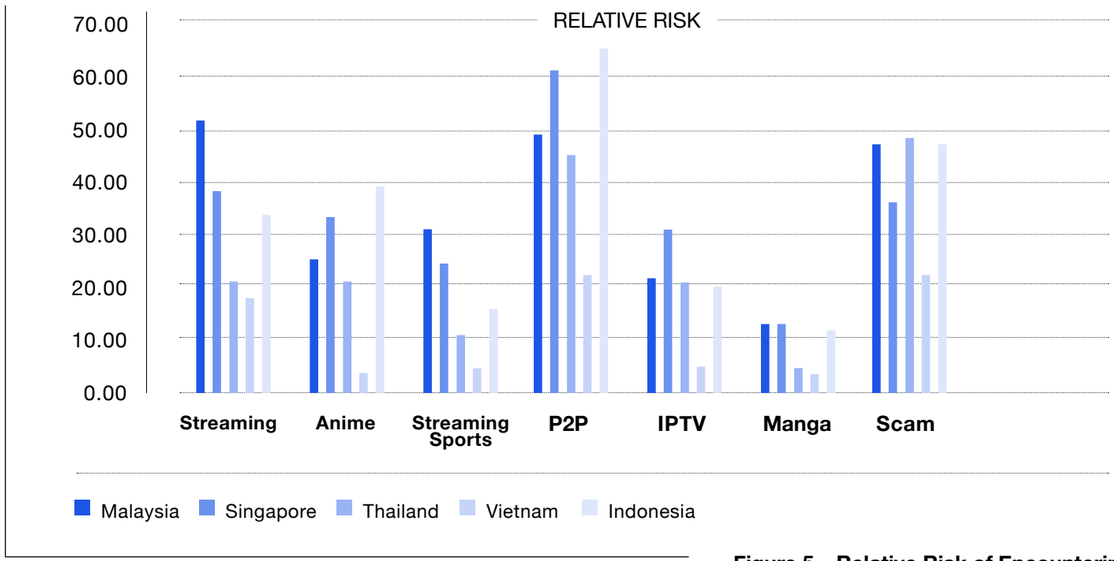


Figure 5 – Relative Risk of Encountering a Cyber Threat by Piracy Type (Worst-Case)

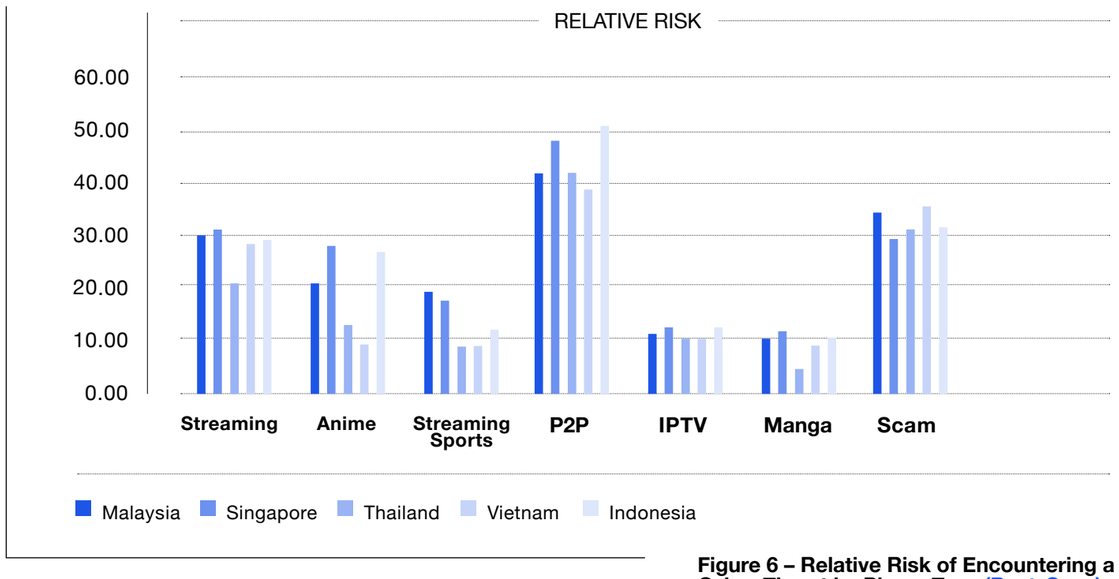


Figure 6 – Relative Risk of Encountering a Cyber Threat by Piracy Type (Best-Case)

Figure 7 shows a heatmap to summarize the worst-case results. The heatmap provides a powerful visual overview of the relative cyber risk associated with different piracy modalities across five Southeast Asian countries. Compared to the raw data table, the heatmap quickly highlights several key patterns:

- **P2P piracy consistently presents the highest risk** across all countries, with exceptionally high values in Singapore and Indonesia.
- **Malaysia exhibits elevated risks across almost all piracy types,** making it a notable outlier for multi-modality threat exposure.
- **Vietnam stands out for its uniformly low risk levels** in every modality, as clearly reflected by the lighter colours throughout its column.
- **Manga and Anime generally pose lower risks** relative to other piracy types, with the exception of a marked spike in Anime risk for Indonesia.
- **Scam sites represent a significant risk in Malaysia, Thailand, and Indonesia**, reinforcing the need for targeted consumer protection strategies.

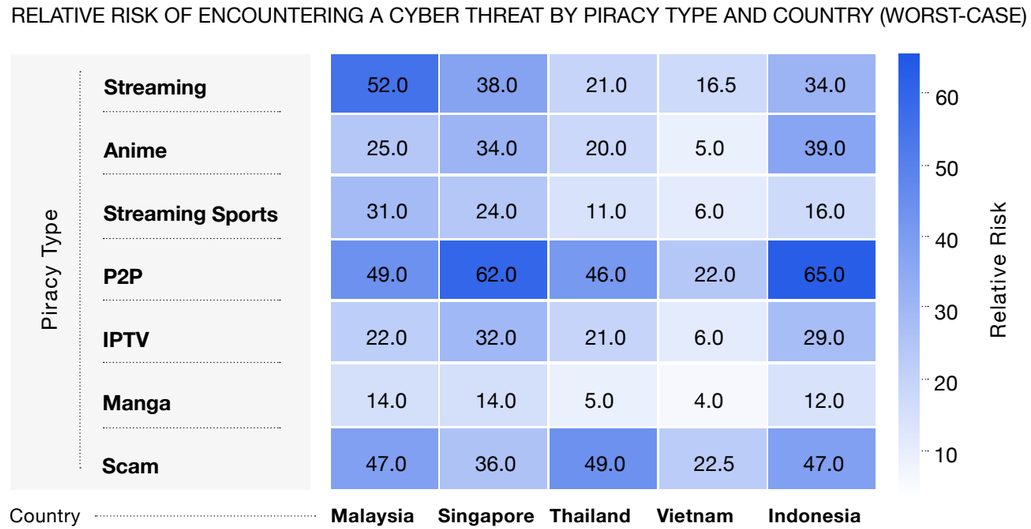


Figure 7 – Relative Risk of Encountering a Cyber Threat by Piracy Type (Worst-Case)

05

Discussion and Conclusions

Implications for Cyber Policy

Frontline Network Defenses

Device and Endpoint Controls

Site Blocking and Takedowns

Discussion and Conclusions

The discussion of these findings begins by re-stating our dual-scenario approach and its rationale. We analyzed 1,200 piracy and mainstream URLs across six cyber-risk categories - malicious, malware, suspicious, phishing, spam and "not recommended" - using reports from over 95 leading threat-intelligence vendors via VirusTotal. To bound uncertainty in vendor overlap, we computed both a "best-case" likelihood (treating all vendors' detections as identifying the same underlying event) and a "worst-case" likelihood (treating each vendor hit as an independent event). This continuity of reporting allows us to present a conservative lower bound and an upper bound on actual exposure, ensuring transparency even as the raw detection counts vary by vendor definitions and database contents.

Turning to the aggregate detection data (Tables 1–4; Figures 3–4), the worst-case scenario yields an overall mean of 26.55 detections per thirty-site sample - peaking at 30 detections each in Malaysia and Singapore - whereas the best-case scenario averages 19.65 detections, with Singapore encountering 22 flagged sites. In both analyses, the highest absolute counts consistently occur in the P2P, Scam and Streaming piracy categories, reflecting the particular attractiveness of P2P swarms, fraudulent portals and unlicensed streaming piracy feeds to threat actors. Likelihood values exceeding one signify that, on average, a consumer will encounter at least one cyber threat when browsing thirty piracy-related sites - a stark contrast to control-group exposures.

When we normalize these findings against the Top 30 mainstream control sites to compute Relative Risk (Tables 5–6; Figures 5–6), the elevation is extraordinary: worst-case RRs for Streaming piracy (e.g. 52.00 in Malaysia), P2P (65.00 in Indonesia) and Scam (49.00 in Thailand) dwarf the control baseline, while best-case RRs remain similarly high (overall average 22.40). Notably, Malaysia and Singapore lead both scenarios, suggesting that jurisdiction-specific factors - such as enforcement rigor, regulatory frameworks and user demand for unlicensed content - drive higher threat densities. The complete absence of detections on control sites in Malaysia, Singapore and Thailand underscores the effectiveness of corporate and government cybersecurity postures in those markets. Finally, our use of a pseudo-count (setting zero detections to one) serves as a standard continuity correction to avoid infinite or undefined RR estimates, stabilizing inter-country comparisons without materially altering the observed risk hierarchy.

IMPLICATIONS FOR CYBER POLICY

The extreme elevation of Relative Risk on piracy-related sites demands that regulators in Singapore, Malaysia, Thailand, Vietnam and Indonesia revisit their domain-blocking frameworks. Rather than relying on static "blacklists" of magistrate-approved piracy domains, governments should mandate dynamic, threat-intel–driven blocking lists - updated in real time with feeds from national CERTs and platforms like VirusTotal - so that newly emerging high-risk URLs (across Streaming piracy, P2P, IPTV, Anime, Manga and Scam categories) can be rapidly sinkholed or filtered at the ISP level. Critically, these measures must be underpinned by transparent administrative processes to prevent broader content censorship.

FRONTLINE NETWORK DEFENSES

ISPs and enterprise network operators should deploy multi-layered filtering, combining DNS-based blocking, TLS/SNI inspection and HTTP(S) reverse-proxy gateways to intercept access to flagged piracy domains. Coupling these with inline threat-intelligence modules - leveraging community-shared indicators of compromise (IoCs) and vendor-agnostic heuristics - allows for both pre-connect blocking of known malicious sites and post-connect identification of suspicious traffic patterns (e.g. cryptojacking or command-and-control callbacks from compromised ISDs). Regular red-teaming and penetration tests against internal networks can validate that blocking rules and detection signatures effectively interdict the full spectrum of piracy-related cyber threats.

DEVICE AND ENDPOINT CONTROLS

Given the persistent risk posed by Illicit Streaming Devices (ISDs) and user-installed P2P/streaming clients, regulators should introduce minimum security standards for consumer electronics - mandating secure boot, signed firmware updates and vulnerability-disclosure policies. Market regulators might require device vendors and online marketplaces to certify that set-top boxes, Android TV apps and torrent clients have undergone independent security audits, with non-compliant products barred from sale or subject to recall. On the endpoint side, enterprises and consumers should adopt next-generation antivirus/EDR solutions tuned to detect both known malware families and heuristic "suspicious" behaviors common to piracy platforms (e.g. unauthorized process injections, post-install persistence).

SITE BLOCKING AND TAKEDOWNS

Implementing dynamic, intelligence-driven site-blocking can sharply reduce consumers' exposure to the elevated cyber risks we observed on piracy platforms. Rather than relying solely on static, judicially-mandated blacklists, Southeast Asian regulators should mandate that ISPs consume real-time feeds from national CERTs and aggregated threat-intelligence sources (e.g. VirusTotal) to automatically sinkhole or filter newly identified high-risk domains across Streaming piracy, Anime, Streaming Sports, P2P, IPTV, Manga and Scam categories. To preserve due-process and public trust, these blocking orders must be subject to transparent administrative review and limited to sites demonstrating a demonstrable pattern of malicious activity. Coupling such site-blocking with user-notification measures - via ISP "walled garden" alerts - and periodic audits of blocklist accuracy will help ensure that legitimate services are not inadvertently censored, while rapidly curtailing consumer access to the most dangerous piracy vectors.

A good example from Australia is shown below in Figure 8 – Telstra (a local ISP) presents warning messages on popups from piracy sites that have been blocked due to malware being detected. It's critical for each entity in the cybersecurity value chain to take proactive steps like this and view digital piracy as a cyber problem to be solved, and not solely through the lens of social and economic losses. Also, recent longitudinal research has indicated that site blocking is effective over the long term within Southeast Asia[32].

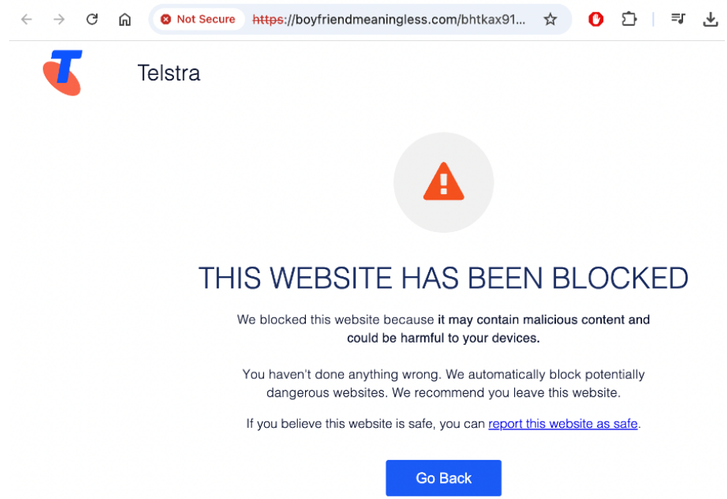


Figure 8 - Example of an ISP blocking message for a malicious pop-up from a piracy site

06

Summary

Summary

Consumers across Southeast Asia are exposed to dramatically elevated cybersecurity risks when accessing digital piracy services. This study's comparative, region-wide analysis demonstrates that piracy sites - including streaming piracy platforms, P2P networks, IPTV services, scam portals, anime, and manga repositories - carry a risk of cyber threat encounters that is, on average, more than 22 times higher than mainstream legal sites. The most hazardous categories are P2P, scam, and piracy streaming services, with relative risks exceeding 30-fold in several countries. In contrast, legitimate platforms in countries such as Malaysia, Singapore, and Indonesia recorded almost no threat detections, highlighting the strong protective effect of established content providers' cybersecurity measures.

The consistently high levels of risk identified across all five countries underscore the urgent need for coordinated responses at both the national and regional levels. The study's findings reinforce the case for proportionate and transparent site-blocking regimes, strengthened law enforcement capability in digital forensics and cyber incident response, and comprehensive public awareness campaigns tailored to local contexts. By implementing these measures, policymakers can help reduce consumer exposure to malware, phishing, scams, and other cyber harms linked to piracy - ultimately protecting digital citizens and supporting the region's growing digital economies.

07

Bibliography

Bibliography

1. Domon, K., Melcarne, A., & Ramello, G. B. (2019). Digital piracy in Asian countries. Journal of Industrial and Business Economics, 46, 117-135.
2. Watters, P. (2021). Consumer Risk and Digital Piracy–Where Does Malware Come From?. Available at SSRN 4536938.
3. Baudach Fernández, S. I. (2023). Streaming Platforms vs. Digital Piracy: A qualitative study on when young adults search for alternatives to stream movies or series online (Bachelor's thesis, University of Twente).
4. Solberg, H. A., Denstadli, J. M., & Nesseler, C. M. (2024). Piracy streaming: How and why a challenge for the sport and media industry. Paper presented at the 32nd European Sport Management Conference, Paris, France.
5. Briel, H., High, M., & Heidingsfelder, M. (Eds.). (2023). The Piracy Years: Internet File Sharing in a Global Context. Liverpool University Press
6. Gopal, R. D., Hojati, A., & Patterson, R. A. (2022). Analysis of third-party request structures to detect fraudulent websites. Decision Support Systems, 154, 113698
7. Federation Against Copyright Theft. (2022, July 21). The hidden dangers of illegal IPTV services: What you need to know. FACT. https://www.fact-uk.org.uk/the-hidden-dangers-of-illegal-iptv-services-what-you-need-to-know/
8. Ristola, J. (2024). Going Gonzo: Crunchyroll, Anime Streaming, and Unpaid Digital Labour. Kinephanos, 10(1), 145-174.
9. Landers, S. (2021). Gotta Catch'Em All!: The National Diet's Inadequate Attempt to Control Manga Pirates. U. Miami L. Rev., 76, 251.
10. Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2019). A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online. In Crime and Society (pp. 91-109). Routledge
11. Eisend, M. (2019). Explaining digital piracy: A meta-analysis. Information Systems Research, 30(2), 636-664
12. Zhai, Y. (2023). Safeguarding Innovation: Exploring the Role of Criminal Justice Systems in Protecting Intellectual Property Rights, Combating Piracy, and Promoting Socio-Economic Stability. International Journal of Criminal Justice Sciences, 18(1), 317-347
13. Domon, K., Melcarne, A., & Ramello, G. B. (2019). Digital piracy in Asian countries. Journal of Industrial and Business Economics, 46(1), 117–135. https://doi.org/10.1007/s40812-019-00111-3
14. Belchior-Rocha, H., Arslan, A., & Yener, S. (2024). Unveiling the ethical dilemmas of digital piracy: A comprehensive exploration of motivations, attitudes, and behaviors. Social Sciences, 13(11), 579. https://doi.org/10.3390/socsci13110579
15. Asia Video Industry Association. (2023, May 25). Piracy steals RM3 billion annually from local content industry. AVIA. https://avia.org/piracy-steals-rm3-billion-annually-from-local-content-industry/
16. Asia Video Industry Association. (2023, August 8). 2023 CAP Consumer Surveys continue to show the benefits of effective site blocking. AVIA. https://avia.org/2023-cap-consumer-surveys-continue-to-show-the-benefits-of-effective-site-blocking/
17. Nguyen, T. H., & Tran, Q. T. (2020). Factors affecting on the digital piracy behavior: An empirical study in Vietnam. Journal of Theoretical and Applied Electronic Commerce Research, 15(2), 67–81. https://doi.org/10.4067/S0718-18762020000200108
18. Lumbanraja, A. U., Nuryakin, C., Muchtar, P. A., Prabowosunu, M. A., Bintara, H., & Permanasari, D. (2018). The economic impact of film piracy: Case study of four metropolitan areas in Indonesia (LPEM UI Working Paper No. 048). Institute for Economic and Social Research, Faculty of Economics and Business, Universitas Indonesia. https://www.lpem.org/repec/lpe/papers/WP201824.pdf
19. Digital Citizens Alliance. (2023, June 8). Piracy subscription services drive credit card fraud and other harms to consumers, new Digital Citizens Alliance investigation and survey finds. https://www.digitalcitizensalliance.org/news/press-releases-2023/piracy-subscription-services-drive-credit-card-fraud-and-other-harms-to-consumers-new-digital-citizens-alliance-investigation-and-survey-finds/
20. Watters, P.A. (2023). Cybercrime and Cybersecurity. CRC Press.
21. Smith, R. G., & Hickman, A. (2022). Estimating the costs of serious and organised crime in Australia, 2020–21. Australian Institute of Criminology

22. Batikas, M., Claussen, J., & Peukert, C. (2019). Follow the money: Online piracy and self-regulation in the advertising industry. International Journal of Industrial Organization, 65, 121-151
23. Goyal, H. (2022). Technology Crime and Organized Syndicates in Cybercrime: Critical Analysis. Issue 5 Int'l JL Mgmt. & Human., 5, 231
24. Rawat, M. (2021). Transnational Cybercrime: Issue of Jurisdiction. Issue 2 Int'l JL Mgmt. & Human., 4, 253
25. The Mirai Botnet – Threats and Mitigations - https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations
26. McKinsey & Company. (2024). Southeast Asia quarterly economic review. https://www.mckinsey.com/featured-insights/future-of-asia/southeast-asia-quarterly-economic-review
27. Department of Foreign Affairs and Trade. (2023). Invested: Australia's Southeast Asia Economic Strategy to 2040 – Chapter 1: Why Southeast Asia? Australian Government. https://www.dfat.gov.au/countries-economies-and-regions/southeast-asia/invested-australias-southeast-asia-economic-strategy-2040/chapter-1-why-southeast-asia
28. The Alliance for Creativity and Entertainment (ACE) is the world's leading coalition dedicated to protecting the legal creative market and reducing digital piracy. Driven by a comprehensive approach to addressing piracy through criminal referrals, civil litigation, and cease-and-desist operations, ACE has achieved many successful global enforcement actions against illegal streaming services and unauthorized content sources and their operators. Drawing upon the collective expertise and resources of more than 50 media and entertainment companies around the world—including sports channels and associations—and reinforced by the Motion Picture Association's content protection operations, ACE protects the creativity and innovation that drives the global growth of core copyright and entertainment industries. The current governing board members for ACE are Amazon, Apple TV+, Netflix, Paramount Global, Sony Pictures, Universal Studios, The Walt Disney Studios, and Warner Bros. Discovery. Charles Rivkin is Chairman and CEO of the Motion Picture Association and Chairman of ACE. For more information, visit www.alliance4creativity.com.
29. For more details of how VirusTotal works, see https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works
30. URL reporting is described in more detail at https://support.virustotal.com/hc/en-us/articles/115002719069-Reports
31. For an explanation of why likelihood is proportional to, but distinct from probability, see https://towardsdatascience.com/likelihood-probability-and-the-math-you-should-know-9bf66db5241b
32. Herps, A., Watters, P., Simone, D., & Foster, J. (2024). When does website blocking actually work? (SSRN Scholarly Paper ID 5238869). SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5238869

08

Appendices

Appendix A – Indonesia Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	9	19	0	1	0	0
Anime	6	12	0	2	2	4
Streaming Sports	3	7	0	0	0	2
P2P	20	24	0	3	0	4
IPTV	5	6	0	2	0	0
Manga	2	8	0	0	0	0
Scam	10	21	0	1	0	0
Control	0	0	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	10	23	0	1	0	0
Anime	9	20	0	4	2	4
Streaming Sports	4	10	0	0	0	2
P2P	22	36	0	3	0	4
IPTV	5	15	0	9	0	0
Manga	2	10	0	0	0	0
Scam	13	33	0	1	0	0
Control	0	0	0	0	0	0

Appendix B – Malaysia Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	6	22	0	2	0	0
Anime	6	9	0	1	1	3
Streaming Sports	8	7	0	2	0	1
P2P	13	23	0	0	0	6
IPTV	5	5	0	1	0	0
Manga	2	9	0	0	0	0
Scam	12	21	0	1	0	0
Control	0	0	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	7	37	0	8	0	0
Anime	7	13	0	1	1	3
Streaming Sports	11	17	0	2	0	1
P2P	13	30	0	0	0	6
IPTV	5	12	0	5	0	0
Manga	2	12	0	0	0	0
Scam	13	33	0	1	0	0
Control	0	0	0	0	0	0

Appendix C – Singapore Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	9	19	0	1	0	2
Anime	9	11	0	1	1	5
Streaming Sports	7	7	0	2	0	0
P2P	16	23	0	1	1	7
IPTV	5	6	0	2	0	0
Manga	3	9	0	0	0	0
Scam	9	19	0	1	0	0
Control	0	0	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	9	26	0	1	0	2
Anime	10	17	0	1	1	5
Streaming Sports	7	15	0	2	0	0
P2P	17	36	0	1	1	7
IPTV	5	16	0	11	0	0
Manga	3	11	0	0	0	0
Scam	11	24	0	1	0	0
Control	0	0	0	0	0	0

Appendix D – Thailand Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	6	9	0	0	0	5
Anime	4	7	0	0	1	2
Streaming Sports	3	4	0	1	1	0
P2P	15	20	0	0	0	7
IPTV	3	5	0	1	1	0
Manga	2	3	0	0	0	0
Scam	7	21	0	3	0	0
Control	0	0	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	6	10	0	0	0	5
Anime	5	12	0	0	1	2
Streaming Sports	4	5	0	1	1	0
P2P	16	23	0	0	0	7
IPTV	3	14	0	3	1	0
Manga	2	3	0	0	0	0
Scam	11	34	0	4	0	0
Control	0	0	0	0	0	0

Appendix E – Vietnam Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	5	19	0	3	0	1
Anime	3	6	0	0	1	0
Streaming Sports	6	2	0	1	1	0
P2P	16	15	0	2	0	6
IPTV	5	5	0	0	1	0
Manga	0	6	0	1	0	1
Scam	11	24	0	0	0	0
Control	0	1	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
Streaming	5	24	0	3	0	1
Anime	3	7	0	0	0	0
Streaming Sports	6	5	0	1	0	0
P2P	16	20	0	2	0	6
IPTV	5	7	0	0	0	0
Manga	0	6	0	1	0	1
Scam	14	31	0	0	0	0
Control	0	2	0	0	0	0

Notes

RESEARCHER BIOGRAPHY

Professor Watters is a trusted cybersecurity researcher and thought leader at Cyberstronomy Pty Ltd. He is the author of *Counterintelligence in a Cyber World* (Springer - ISBN 978-3031352867) and *Cybercrime and Cybersecurity* (CRC Press - ISBN 978-1032524511). Professor Watters is Honorary Professor of Security Studies and Criminology at Macquarie University, and Professor of Information Systems at Holmesglen Institute. His work has been cited 10,674 times, with an *h*-index of 49, and an *i*-10 index of 144. He was ranked within the top 0.5% of researchers worldwide (all fields) by ScholarGPS in 2024.

ACKNOWLEDGEMENTS

Funding for this research was provided by the Motion Picture Association. The work was produced independently by Dr Paul Watters, Macquarie University (Sydney).