Consumer Risk from Piracy in Poland

Paul A. Watters PhD
Adjunct Professor of Cybersecurity, La Trobe University (Melbourne)
Honorary Professor of Security Studies and Criminology, Macquarie University (Sydney)

Consumer Risk from Piracy in Poland

Consumer Risk from Piracy in Poland

Executive Summary

Consumers in Poland who access piracy sites and services are at severe risk of cyber threats from a range of criminal groups running said digital piracy services against a complex and challenging geopolitical landscape. Piracy sites frequently harbor concealed malware or viruses, posing a threat to users who may inadvertently infect their devices, leading to personal information theft, file damage, ransomware, sextortion, or system hijacking.

This study aimed to quantify the cyber risk for Polish consumers using digital piracy websites (including fraudulent sites), illegal streaming sites, or IPTV services. When compared to a set of mainstream control sites, the relative risk was 38.50 for peer-to-peer (P2P) sites, 25.50 for streaming sites, 9.00 for fraudulent sites, and 7.50 for IPTV sites. In simple terms, consumers are up to 38.50 times more likely to encounter a cyber threat when using P2P sites in Poland compared to mainstream websites in the control group, which is an extraordinary result. The relative risk has the same interpretation for streaming, fraudulent, and IPTV sites, with consumers being up to 25.50, 9.00 and 7.50 times more likely to encounter a cyber threat, respectively, when compared to the control group.

To counter the elevated cyber risk, this report recommends immediate action:

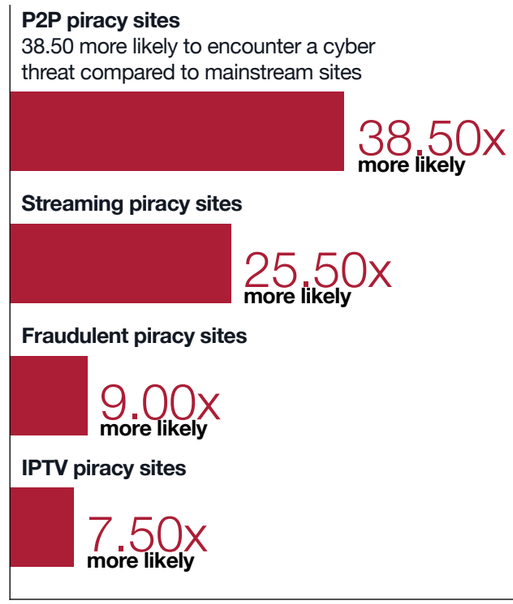
1. Implement proportionate and transparent administrative site blocking of piracy sites and services.

2. Increase funding for Polish law enforcement to develop further capability in digital forensics and incident response to deal with the heightened cyber threats arising from the confluence of digital piracy and cyber threats; and

3. Develop a national awareness and education campaign in Poland specifically targeting cyber threats from piracy sites or services.

These recommendations form a sensible and commensurate response to a serious threat to consumer safety, especially in an era when data breaches and large-scale identity theft have become the international norm.

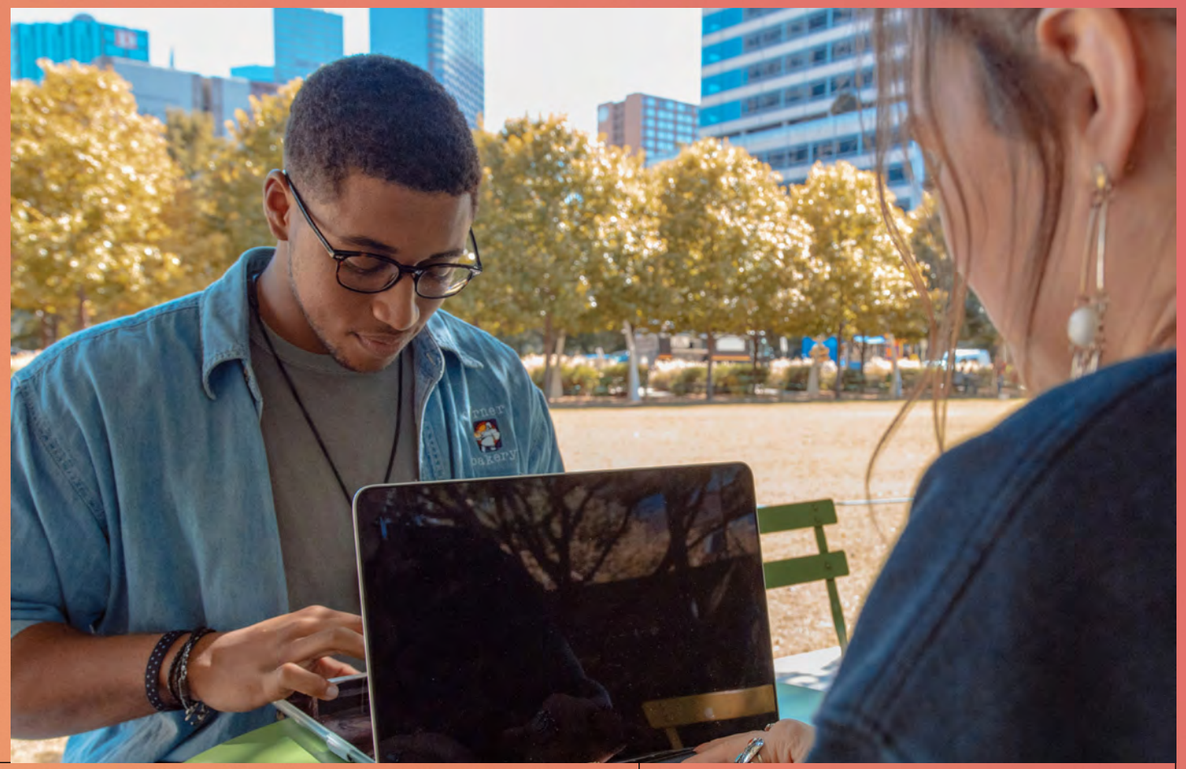
Polish consumers are more likely to encounter a cyber threat when using piracy sites:



Contents

Consumer Risk from Piracy in Poland

Introduction



01

What is digital piracy?

What are the social and economic consequences of digital piracy?

What are the consumer risks of digital piracy?

What is the consumer threat model for piracy?

An evolving threat model for digital piracy?

What is the financial situation of consumers in Poland?

Why are Polish consumers attractive targets for cyber threats?

What are the protective factors in terms of cyber policy and regulatory responses?

Introduction

According to the Polish Cyberspace Defense Forces, Poland is the country with the most cyber attacks in the world.[1] This research examines the repercussions of digital piracy on consumers in Poland, particularly in the realm of cybersecurity risks. The primary objective is to gather evidence to make recommendations to address the interconnected challenges posed by digital piracy and cybersecurity, ultimately ensuring the protection of both consumers and the digital landscape.

Specifically, the study thoroughly explores consumer risk, identifies actual vulnerabilities, and a comprehensive risk assessment. Only after understanding these aspects can effective approaches to risk mitigation—including regulatory reforms, allocation of resources for law enforcement, and consumer education—be developed. Utilizing an empirical methodology, the research aims to provide scientific insights into the core research question: what is the cyber risk for consumers in Poland from visiting piracy sites?

What is digital piracy?

Digital piracy involves the unauthorized utilization, reproduction, distribution, or downloading of copyrighted materials, encompassing movies, music, software, or books, without the explicit consent of the copyright holder.[2]

Essentially, it entails acquiring or distributing copyrighted content without proper payment or authorization. Within Poland, four predominant types of digital piracy services operate:

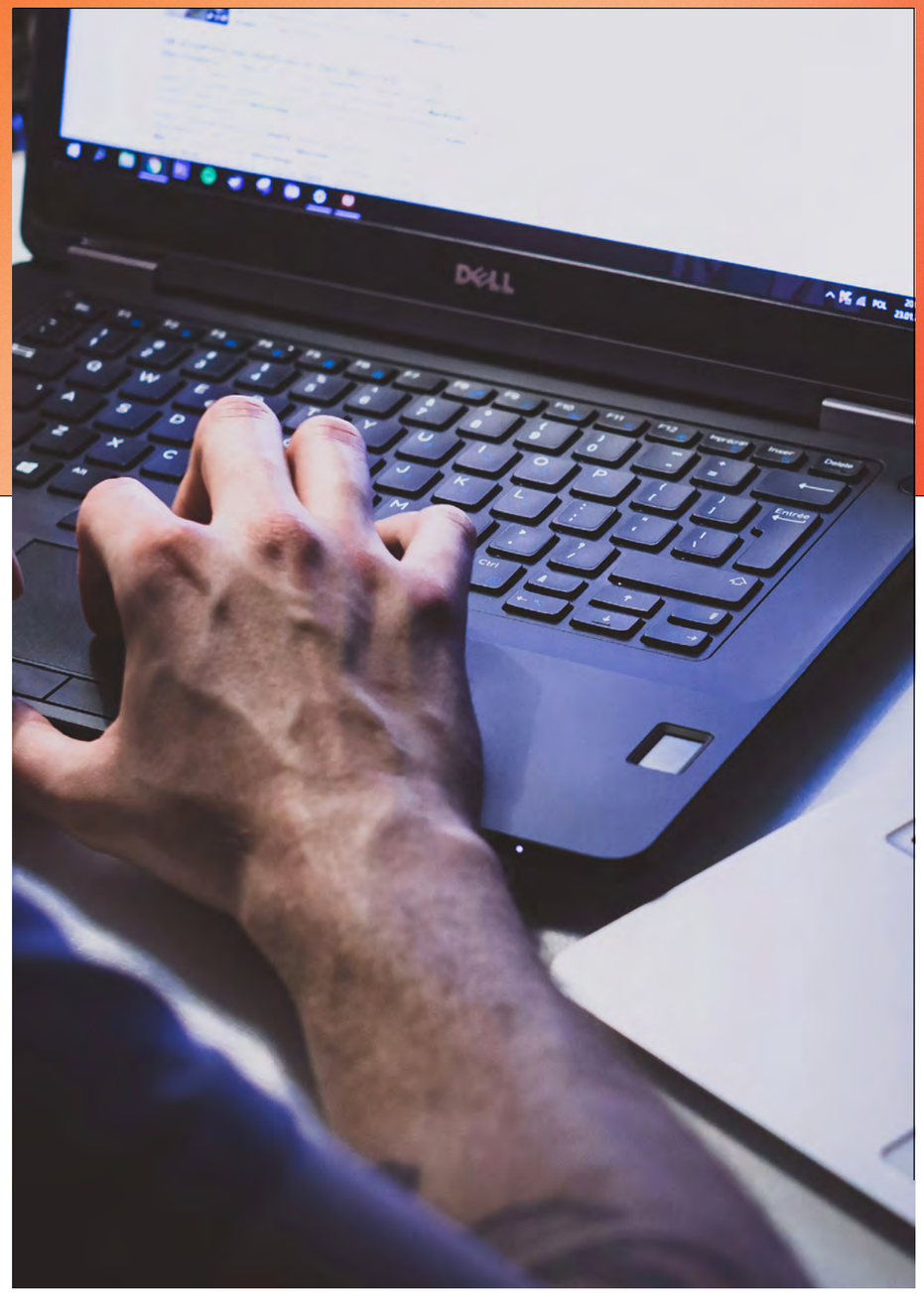
- IPTV subscription services
- illicit streaming sites
- P2P sites
- fraudulent piracy sites.

Each category exhibits distinct operating models, technical implementations, and illicit business drivers. IPTV subscription services often necessitate a subscription fee, providing access to live channels, films, TV shows, sports content, and sometimes video on demand (VOD) without remitting revenue to rightsholders. P2P networks facilitate direct file sharing among users in a decentralized manner. Illicit streaming involves real-time access to content without downloading the entire file, often using subscription-based or ad-supported models.

Fraudulent piracy sites deceive users by presenting pirated content as legitimate, tricking them into payments or downloading malicious software. These activities not only violate content creators' rights but also carry legal consequences for both distributors and consumers. Illicit file sharing and streaming contribute to a broader online cybercrime ecosystem, where operators gain substantial financial benefits, often alongside other illicit services such as hacking and child exploitation. Deloitte (2023) reports that in Poland, 7.3 million consumers visit piracy sites—no legal alternative in Poland comes close to having this number of subscribers.[3] The number of illicit streaming VOD services available in Poland is the second largest in Europe, with an average of 129.3 million monthly visits to pirate sites.

Compared to other markets, legitimate IPTV penetration in Poland is the third lowest in Europe.

As illustrated in this report—and from previous research[4]—there are also direct consumer impacts from using digital piracy services, such as malware infections, leading to personal data theft and subsequent identity fraud. These impacts make preventing access to digital piracy so important—it prevents consumers from becoming victims.



What are the social and economic consequences of digital piracy?

Digital piracy has wide-ranging social consequences, eroding intellectual property rights, impacting employment, diminishing content quality and diversity, and carrying legal implications. On the economic front, it results in revenue loss for creators, reduced investment in innovation, negative industry impacts, increased cybersecurity costs, and a global economic footprint affecting international trade relations.

The overall effect is a pervasive undermining of creative industries, discouragement of investment, and challenges to maintaining cultural diversity, calling for comprehensive strategies that involve legal measures, industry collaboration, consumer education, and innovative business models to mitigate these social and economic consequences. Previous research in Poland has indicated a link between risky behaviors in cyberspace and the use of digital piracy services;[5] providing further education and awareness about the consequences—one of the recommendations in this report—was also supported by this qualitative project. As indicated in the Deloitte report, the economic consequences are severe—PLN7.36b of pirated content is consumed annually, with PLN1.86b lost to the state budget in foregone taxation. Ironically, the average monthly expenditure on pirated content is PLN57, combining live streaming and VOD content. This financial impact diverts critical funding away from investment into local creative content and potential taxation revenue that could fund the construction of hospitals and schools. The full social and economic consequences are described below.

SOCIAL CONSEQUENCES

Digital piracy undermines the value of intellectual property, discouraging innovation and creativity by diminishing the rewards for content creators. It is also worth emphasizing that the entertainment and software industries are major contributors to employment. Digital piracy can lead to job losses, affecting individuals involved in content creation, distribution, and related direct and indirect services.

The unauthorized distribution of cultural works can dilute cultural diversity as it may discourage local creators who fail to recoup their initial investment from producing further content that represents their unique perspectives and storytelling.

Also, individuals involved in digital piracy may face legal repercussions, potentially leading to fines, penalties, or imprisonment, contributing to an overall breakdown of law and order in the digital domain. While some critical theorists have branded pirates as “amateur archivists” who are simply preserving cultural artifacts in the face of the “collapse of modern industrialized society,”[6] the actual consequences of not supporting anti-piracy efforts have a clear and measurable impact on fostering cultural production.

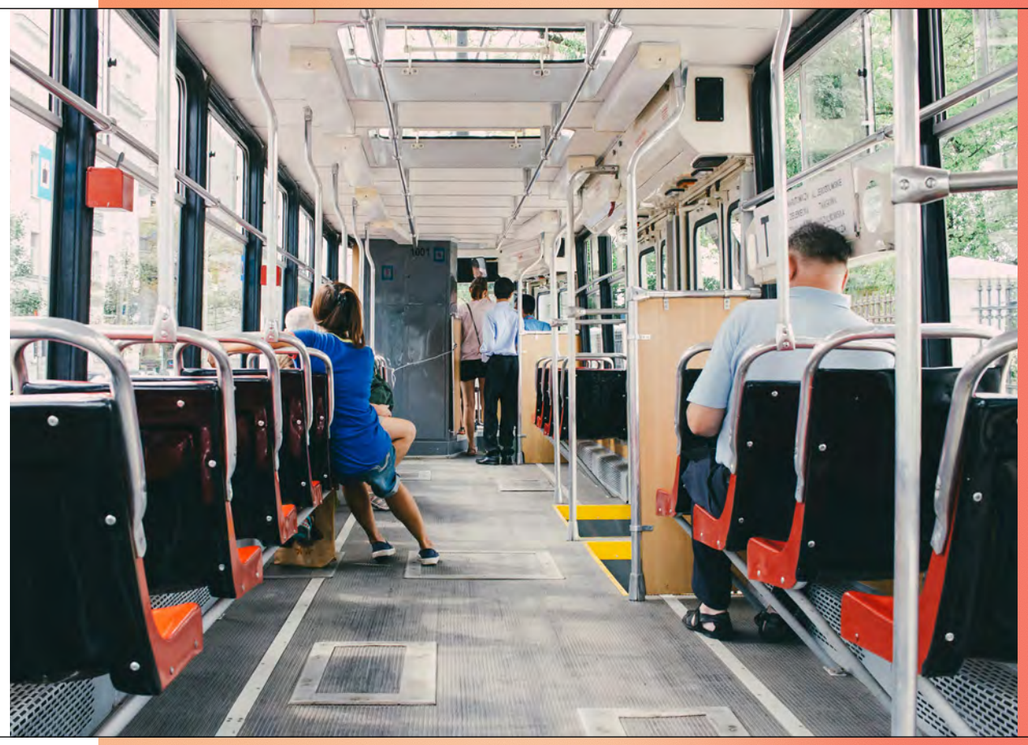
ECONOMIC CONSEQUENCES

Piracy directly impacts the revenue streams of content creators, as they lose potential earnings when consumers access their work without proper compensation. Piracy can also deter investors from supporting creative projects, as the risk of financial returns decreases when content is susceptible to widespread unauthorized distribution. Industries such as film, software, music, and publishing can experience significant revenue decline, affecting not only creators, but also distributors, retailers, and other related direct and indirect businesses.[7] As the Deloitte report highlights, the direct impact on cultural production is apparent when you compare the Polish Film Institute’s budget of PLN420m with the combined financial impact of illegal VOD and live streaming, IPTV, and satellite card sharing being PLN3b.

In addition, businesses may need to invest more in proactive cybersecurity measures to protect their digital assets from piracy, increasing operational costs.[8] Finally, digital piracy has a global economic impact, affecting international trade relations as countries seek to address intellectual property violations through trade agreements and negotiations.

What are the consumer risks of digital piracy?

Consumer risks linked to digital piracy, especially concerning cybersecurity, encompass cyber threats like malware and viruses, identity theft, data breaches, legal consequences, piracy compromise, and financial losses. Pirated content frequently harbors concealed malware or viruses, posing a threat to users who may inadvertently infect their devices, leading to personal information theft, file damage, ransomware, sextortion, or system hijacking.[9]



Certain pirated platforms employ deceptive tactics to extract user data, potentially resulting in identity theft, phishing, or ransomware attacks.[10] Engaging with unauthorized sources for software or content exposes users to data breaches, compromising sensitive information, and those involved in piracy may face legal repercussions, disrupting both personal and professional aspects of their lives. Additionally, piracy activities jeopardize user privacy, with illegitimate platforms collecting and misusing data without consent, often leading to privacy breaches.[11] With relatively high global per capita gross domestic product (GDP), Polish consumers become attractive targets for commercial-scale piracy crime groups due to substantial profits and relatively low risks. Organized crime groups exploit piracy sites for revenue through advertising, subscriptions, or direct sales of pirated content, often using these platforms for money laundering.[12] These groups collaborate with cybercriminals, exploit global internet dynamics, and navigate legal loopholes across borders, presenting challenges for law enforcement agencies in effectively combating these sophisticated operations.[13]

What is the consumer threat model for piracy?

A threat model seeks to recognize and assess potential threats, examining the probable attack vectors employed by malicious actors in a specific context. With the emergence of a range of piracy services, the risk landscape for consumers, their employers, and the state has undergone alterations and intensified. Some of these evolving dynamics are described below.

As mentioned earlier, Polish Cyberspace Defense Forces report that Poland is currently the country with the most cyber attacks in the world,[14] so the cyber risks arising from digital piracy must be understood in this context, especially the distribution and proliferation of malware.

ILLICIT STREAMING SERVICES

Illicit streaming involves real-time access to content without downloading the entire file, often using subscription-based or ad-supported business models.[15] Such illicit sites offer content that typically includes live film/TV and sports channels. These services may also include some VOD. Consumers pay a single subscription fee to access multiple paid services; however, the revenue is not paid to rightsholders. They often rely on advertising revenue, exposing users to potentially harmful ads or pop-ups that may contain malware or phishing links. Some streaming platforms falsely promise free access to premium content, tricking users into providing personal or financial information for supposed subscriptions, leading to scams and identity theft.

PEER-TO-PEER (P2P) NETWORKS

P2P networks[16] are systems where users can share files directly with each other. It is a decentralized way of sharing files, allowing individuals to upload and download content directly from other users' computers. They can be breeding grounds for malware, where files shared may contain hidden malicious software that can compromise users' devices and steal personal information, including malvertizing, as shown in Figure 1.

Figure 1 – Traditional Piracy Threat Model

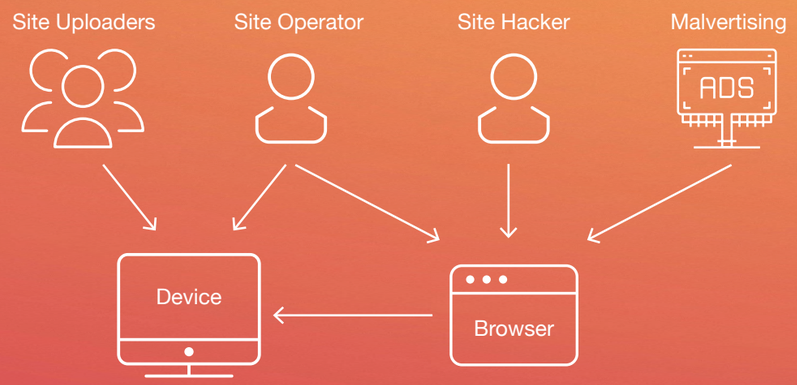
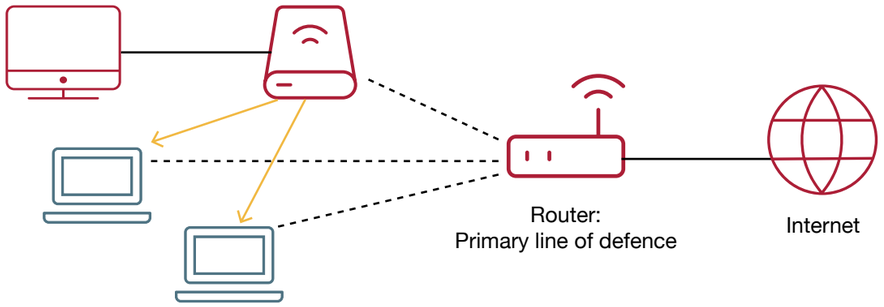


Figure 2 – Threat Model – IPTV Subscription Services

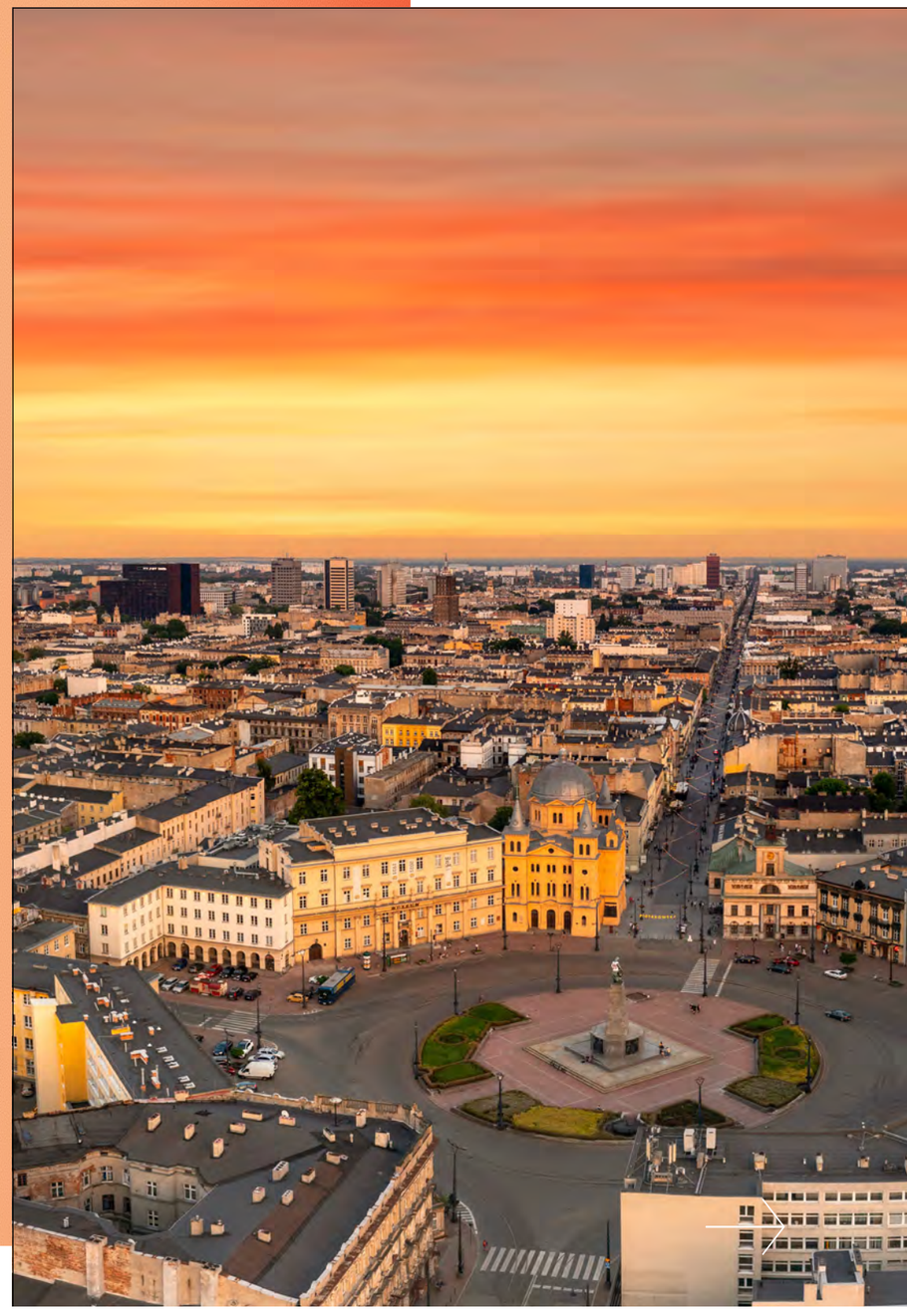


IPTV SUBSCRIPTION SERVICES

IPTV subscription services[17] are piracy services that require a subscription fee and offer content, including live channels of film/TV and sports content. These services may also include some VOD. Typically, consumers pay a single subscription fee to access multiple paid services; however, the revenue is not paid to rightsholders. They usually require payment and often pose the risk of financial loss, where users pay for access to content without the revenue reaching the rightful content owners. Also, users may be required to provide sensitive financial information for subscriptions, making them vulnerable to payment fraud or unauthorized access to their financial accounts, as proven in a recent study by the Digital Citizens Alliance.[18] The threat model is summarized in Figure 2.

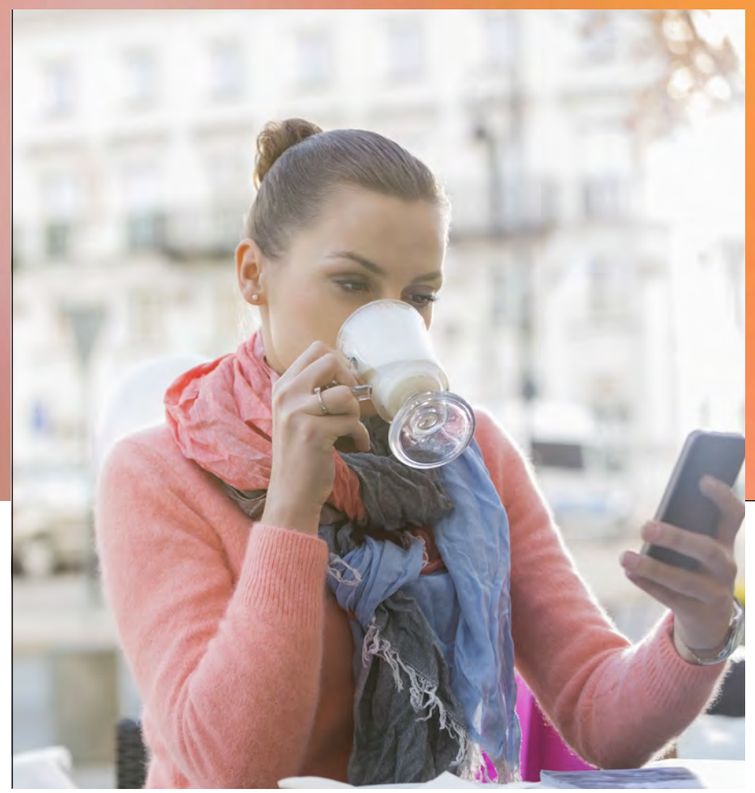
FRAUDULENT PIRACY SITES

Fraudulent piracy sites are websites that deceive users by impersonating piracy sites in order to scam them. The fraudulent sites identified in the study are similarly formatted and advertised on the page. Sometimes, they even have domain names that are analogous to those of other popular piracy sites. However, the user will discover that they will not be able to access the advertised pirated content with the intention of the site to steal the users' credit card and/or personal details. These sites appear to offer pirated content, tricking users into paying for access or downloading malicious software. Fraudulent piracy sites do not host any content; instead, they may trick users into purchasing overpriced subscriptions after acquiring their credit card details. They may deceive users into providing personal information, leading to identity theft or phishing attacks where cybercriminals exploit the acquired data for malicious purposes. Fraudulent sites can trick users into paying for access to content or services that are not delivered as promised, resulting in financial losses without obtaining the advertised material.



An evolving threat model for digital piracy?

As technology advances and user behavior shifts, the threat landscape evolves, demanding a nuanced understanding of emerging risks.[19] Malicious actors commonly distribute malware through pirated content, posing risks of infecting users' devices and compromising personal data. The sophistication of malware distribution techniques is rising, with attackers leveraging advanced methods such as polymorphic malware to evade traditional security measures.



Consumers may fall victim to subscription scams on fraudulent sites, paying for illegitimate services or providing financial information to fraudulent platforms. Scammers and hackers increasingly employ deceptive tactics, mimicking legitimate subscription models, making it harder for users to distinguish between authentic and fraudulent services. Illicit streaming platforms have historically collected and misused user data without consent, leading to privacy breaches. With the advent of more advanced tracking technologies, the scope of privacy breaches has expanded, encompassing more intricate profiling and potential exploitation of personal information.

The unauthorized distribution of copyrighted material may have economic implications. As organized crime groups increasingly exploit IPTV services for financial gain, the threat to national security has evolved, necessitating a broader understanding of the economic, social, and geopolitical impacts.

However, in Poland, the government and content creators are intensifying efforts to combat piracy, leading to increased legal scrutiny and potential legal actions against users involved in unauthorized streaming or distribution.[20]

Across all these services, consumers supplying their personal data may lead to privacy breaches, where user data is collected and misused without consent, compromising individual privacy. Also, unauthorized sources and fraudulent sites may be involved in data breaches, exposing sensitive information, including financial details and passwords, to potential exploitation. Understanding this threat model is crucial for consumers to make informed decisions, adopt secure online practices, and be vigilant against the potential risks associated with P2P, illicit streaming, IPTV, and fraudulent sites.

What is the financial situation of consumers in Poland?

Poland is one of the most populous countries in Europe, with a population that has been relatively stable (37,550,000).[21] Poland has a reasonably tech-savvy population, with widespread internet use and technology adoption. This influences how individuals access financial services, engage in online banking, and make digital transactions.

International Monetary Fund data indicate a GDP of US$880b, GDP growth of 2.3 percent, and GDP per capita of US$23,430. Unemployment is very low, at 2.9 percent.

Poland had experienced steady economic growth in the years leading up to 2024. However, the COVID-19 pandemic did have some impact on the economy, as it did globally. Like other countries, Poland's economic performance was influenced by various factors, including government policies, global economic conditions, and the effectiveness of pandemic-related measures. Poland had relatively low unemployment rates compared to some other European countries. However, the labor market situation can change, and fluctuations may occur based on economic conditions and various external factors.

Income levels in Poland varied among different segments of the population. Urban areas generally had higher income levels compared to rural areas. The distribution of income and wealth significantly affects consumers' financial situation. The cost of living in Poland was generally lower than in many Western European countries, making it relatively affordable for residents. Government policies and support programs, especially those introduced in response to the COVID-19 pandemic, played a role in mitigating economic challenges for individuals and businesses.

Why are Polish consumers attractive targets for cyber threats?

Poland has experienced significant economic growth and digital transformation in recent years. Increased digitization and technology adoption in various aspects of daily life make consumers more reliant on digital platforms, potentially providing more opportunities for cybercriminals. With the growth of online banking and electronic financial transactions, Polish consumers are more likely to conduct financial activities over the internet. Cybercriminals often target individuals engaged in online banking to gain unauthorized access to financial accounts or conduct fraudulent transactions.

The popularity of e-commerce and online shopping in Poland provides cybercriminals with opportunities to exploit vulnerabilities in online payment systems, compromise user accounts, or engage in phishing attacks targeting individuals making online purchases. Also, Poland has a relatively high internet penetration rate, and consumers are actively engaged in online activities, including social media, email communication, and accessing various online services. The large user base presents a broader attack surface for cyber threats.

Cybercriminals may see potential financial gains in targeting Polish consumers with ransomware attacks or exploiting data breaches. The compromise of personal information, including financial data and sensitive details, can be lucrative on the black market. While awareness of cybersecurity has increased, there may still be variations in the level of awareness and cybersecurity practices among the general population.[22] Cybercriminals often exploit security weaknesses resulting from poor cybersecurity hygiene, such as using weak passwords or falling for phishing scams.

In some cases, cyber threats may be motivated by geopolitical factors. Poland's geopolitical position and its relationships with neighboring countries could make it a target for cyber activities driven by political motivations. Beyond consumer targeting, there may be cyber threats to disrupt critical infrastructure or industrial systems within the country. Such threats could have broader implications for national security and the economy.

An international survey of cybercrime prevalence in Europe found that over the span of five years, Polish consumers had the highest rate of malware infection (68.10% of consumers),[23] with 13.9 percent of Polish respondents suffering an associated cybercrime, including bank fraud, online shopping fraud, extortion, or scams. Polish consumers are also paying the highest cost for protection from consumer-focused cybercrime,[24] at approximately 50 Euros per capita.

What are the protective factors in terms of cyber policy and regulatory responses?

As an European Union (EU) member state, Poland is subject to both EU-wide regulations and national policies aimed at enhancing cybersecurity and protecting against cyber threats. The protective factors in terms of cyber policy and regulatory responses in Poland include a combination of EU-level initiatives and domestic measures.

Poland's National Cybersecurity Strategy outlines the country's approach to addressing cyber threats.[26] The strategy includes enhancing cybersecurity capabilities, promoting information sharing, and strengthening cooperation between public and private sectors. The National Cybersecurity Center in Poland[27] is crucial in coordinating and implementing cybersecurity measures. It is a focal point for information exchange, incident response, and collaboration between various stakeholders.

Poland has a Computer Security Incident Response Team (CSIRT) responsible for coordinating responses to cybersecurity incidents.[28] CSIRT provides expertise, guidance, and support to both public and private entities, contributing to the country's overall cyber resilience.

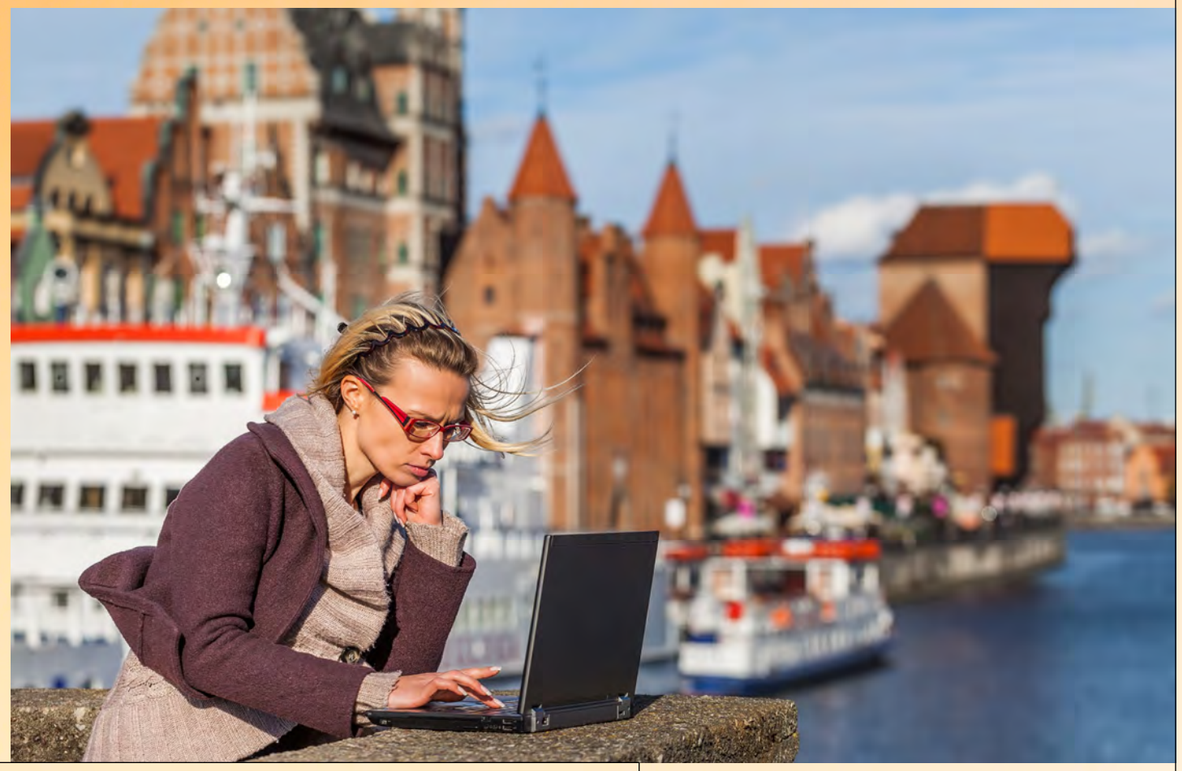
Poland has enacted specific legislation addressing cybersecurity and cybercrime.[29] The legal framework includes provisions to prosecute cybercriminals, protect critical infrastructure, and safeguard sensitive information. Poland adheres to the European Cybersecurity Certification Framework[30] as part of the EU Cybersecurity Act. This framework establishes a common set of rules for certifying the cybersecurity of products, processes, and services, promoting a higher level of cybersecurity across the EU.

Poland actively participates in EU-level initiatives aimed at enhancing cybersecurity cooperation and resilience. This includes collaboration with EU agencies, such as the European Union Agency for Cybersecurity (ENISA),[31] and participation in joint cybersecurity exercises with NATO.[32]

Public-private collaboration is emphasized in Poland's cybersecurity approach. Cooperation between government entities, businesses, and academic institutions is essential for sharing threat intelligence and best practices and collectively addressing cybersecurity challenges. Improving cybersecurity education and awareness is integral to Poland's protective measures.[33] Public awareness campaigns and educational programs aim to enhance cybersecurity practices among individuals, businesses, and organizations.

In summary, Poland has a mature and well-developed set of defenses against cyber attacks. However, current data indicates a very high level of cyber risk, and digital piracy sites are one very attractive route to targeting Polish consumers with very sophisticated cyber attacks. This study will quantify the increased level of cyber risk associated with visiting a range of the most popular digital piracy sites in Poland and provide an estimate of the relative cyber risk compared to visiting the most popular non-piracy (mainstream) websites.

Methods



02

Methods

Data were gathered from Poland to assess cyber risks associated with piracy websites. The evaluation method relied on VirusTotal, a Google tool for scanning websites for malware, phishing, and suspicious, malicious or spam content.

VirusTotal cross-references information from over 90 antivirus vendors and executes potentially harmful code in a secure environment to identify threats, making it a widely acknowledged tool in antivirus research globally. The data collected from VirusTotal was instrumental in establishing risk metrics, including the likelihood of encountering threats in comparison to safe mainstream sites.

The Alliance for Creativity and Entertainment (ACE),[34] a prominent anti-piracy association, supplied a list of piracy websites offering unauthorized film and TV content and fraudulent sites popular in Poland. ACE compiled this list based on copyright removal requests, site blocks in various countries, and other reliable sources. Specific samples were chosen from this list for comparative analysis. Further, a control sample from each country's top 30 most popular websites was evaluated to ensure a valid comparison between piracy sites and typical websites. Each sample consisted of 30 sites, allowing for reliable population inferences using the sample standard deviation to calculate the standard error. This method ensured representative samples and an experimental design with controls for drawing valid conclusions. In cases where a piracy site overlapped with the control sample, the next most popular site in the top sites list for that country was substituted.

SAMPLES FOR SPECIFIC CATEGORIES BASED ON CONSUMERS' SITE VISITS IN FEBRUARY 2024 IN POLAND WERE GATHERED AS FOLLOWS:

- The top 30 IPTV subscription service sites
- The top 30 streaming piracy sites
- The top 30 P2P piracy sites
- The top 30 fraudulent piracy sites.

Throughout the sampling period, the term "top 30" denoted the most frequently visited P2P and streaming sites, aligning with the Pareto principle, suggesting that a small number of sites likely account for the most traffic.

Notably, the fraudulent piracy sites, independently verified by ACE, did not actually host pirated content. Making a clear distinction between piracy and fraudulent piracy sites was considered crucial. Fraudulent piracy sites do not host content; instead, they trick users into purchasing overpriced subscriptions after acquiring their credit card details. While all piracy sites entail risks, fraudulent sites were anticipated to pose an even greater risk due to their deceptive nature.

Results

03

Worst Case and Best Case Likelihood Scenarios

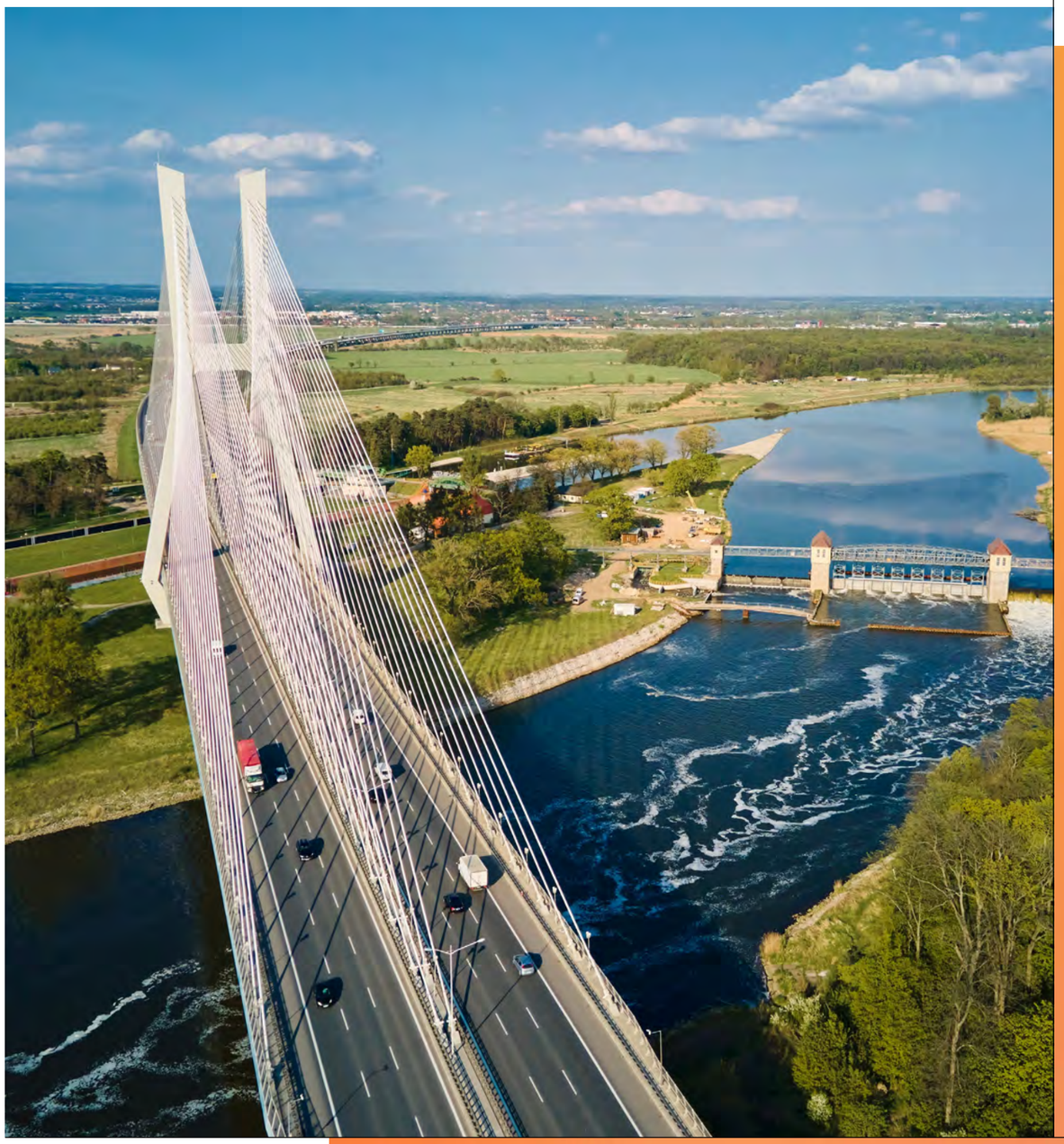
Results

The website URLs from the sample—consisting of 150 sites distributed across five categories (IPTV subscription services, top 30 streaming, top 30 P2P, top 30 fraudulent, and control) and spanning five countries—were submitted to VirusTotal.

The outcomes were systematically organized, presenting data across six cyber risk categories: malicious, malware, suspicious, phishing, spam, and not recommended. The delineation of these categories can be specified as follows:[35]

- **Malicious –** confirmed by a human assessment that a site harbors cyber threats.
- **Suspicious –** identified through machine detection indicating the presence of cyber threats on a site.
- **Malware –** denotes the distribution of malware originating from the site.
- **Phishing –** indicates that the site is employed to obtain users' credentials illicitly.
- **Spam –** signifies that the site is utilized for unsolicited emails, pop-ups, and automated commenting.
- **Not recommended –** implies potential distribution of unwanted software.

These classifications derive from reports provided by over 90 partners, including the world's largest cybersecurity threat detection companies. They signify a collaborative initiative within the community to pinpoint websites actively involved in disseminating cyber threats. Each detection company reports only one category per site, reflecting their evaluation of the risks associated with the respective site.



Worst Case and Best Case Likelihood Scenarios

We offer a worst-case and best-case likelihood estimate in each analysis due to the independent reports from multiple antivirus vendors on VirusTotal. Given that each antivirus vendor employs distinct definitions and maintains proprietary threat databases, the best-case estimate takes a highly conservative approach, assuming all detections from each vendor identify the same malware sample.

Conversely, the worst-case estimate assumes that each vendor identifies entirely different samples. Examining the threat reports reveals that most detections are distinct, so we provide this range for transparency.

Tables 1 and 2 showcase the worst-case and best-case results for P2P, streaming, fraudulent, and the control group in Poland. In the worst case, the estimates suggest the average likelihood of encountering a cyber threat on a top 30 P2P site was 2.56, a top 30 streaming site was 1.70, an IPTV site was 0.50, and a top 30 fraudulent sites was 0.60. Control sites were 0.06. In the best case, P2P sites were 1.60, streaming sites were 0.93, IPTV sites were 0.43, and fraudulent sites were 0.30. The control results remained consistent in both the best and worst cases.[36]

In simple terms, where the likelihood is greater than one, consumers are, on average, likely to encounter one cyber threat. Using a control set of mainstream websites, we can calculate how elevated this risk is compared to normal browsing.

For example, an average likelihood of 2.56 means that for every piracy site visited, a consumer is exposed to an average of 2.56 cyber threats per site, which is very high. In other words, statistically, each visit to a pirate site entails a user being exposed to 2.56 threats. For IPTV, it is crucial to note that this analysis only scrutinized the landing pages of IPTV subscription services, not the IPTV service itself, as malware could also be present in the specialized software for each platform.

In basic terms, if the likelihood is higher than one, consumers are expected to encounter at least one cyber threat on average. We use a control group of popular websites to measure how much higher this risk is compared to regular browsing. Table 3 presents the relative risk calculation, which involves dividing the average detection data by the detection value of the control group for both the best-case and worst-case likelihood estimates. Compared to a set of mainstream controls, the relative risk was 38.50 for P2P sites, 25.50 for streaming sites, 9.00 for fraudulent sites, and 7.50 for IPTV sites. Put simply, consumers are up to 38.50 times more likely to encounter a cyber threat when using piracy sites or services in Poland, which is very high.

Table 1 – Worst-case scenario—Average likelihood of all cyber threats

Illegal IPTV

Country	N	Detections	Likelihood
Poland	30	15	0.50

Streaming

Country	N	Detections	Likelihood
Poland	30	51	1.70

P2P

Country	N	Detections	Likelihood
Poland	30	77	2.56

Fraudulent

Country	N	Detections	Likelihood
Poland	30	18	0.60

Control

Country	N	Detections	Likelihood
Poland	30	2	0.06

Table 2 – Best-case scenario—Average likelihood of all cyber threats

Illegal IPTV

Country	N	Detections	Likelihood
Poland	30	13	0.43

Streaming

Country	N	Detections	Likelihood
Poland	30	28	0.93

P2P

Country	N	Detections	Likelihood
Poland	30	48	1.60

Fraudulent

Country	N	Detections	Likelihood
Poland	30	9	0.30

Control

Country	N	Detections	Likelihood
Poland	30	2	0.06

Table 3 – Relative risk calculations

Worst-Case Scenario

Country	Illegal IPTV	Streaming	P2P	Fraud	Average
Poland	7.50	25.50	38.50	9.00	20.13

Best-Case Scenario

Country	Illegal IPTV	Streaming	P2P	Fraud	Average
Poland	6.50	14.00	24.00	2.00	11.63

Discussion

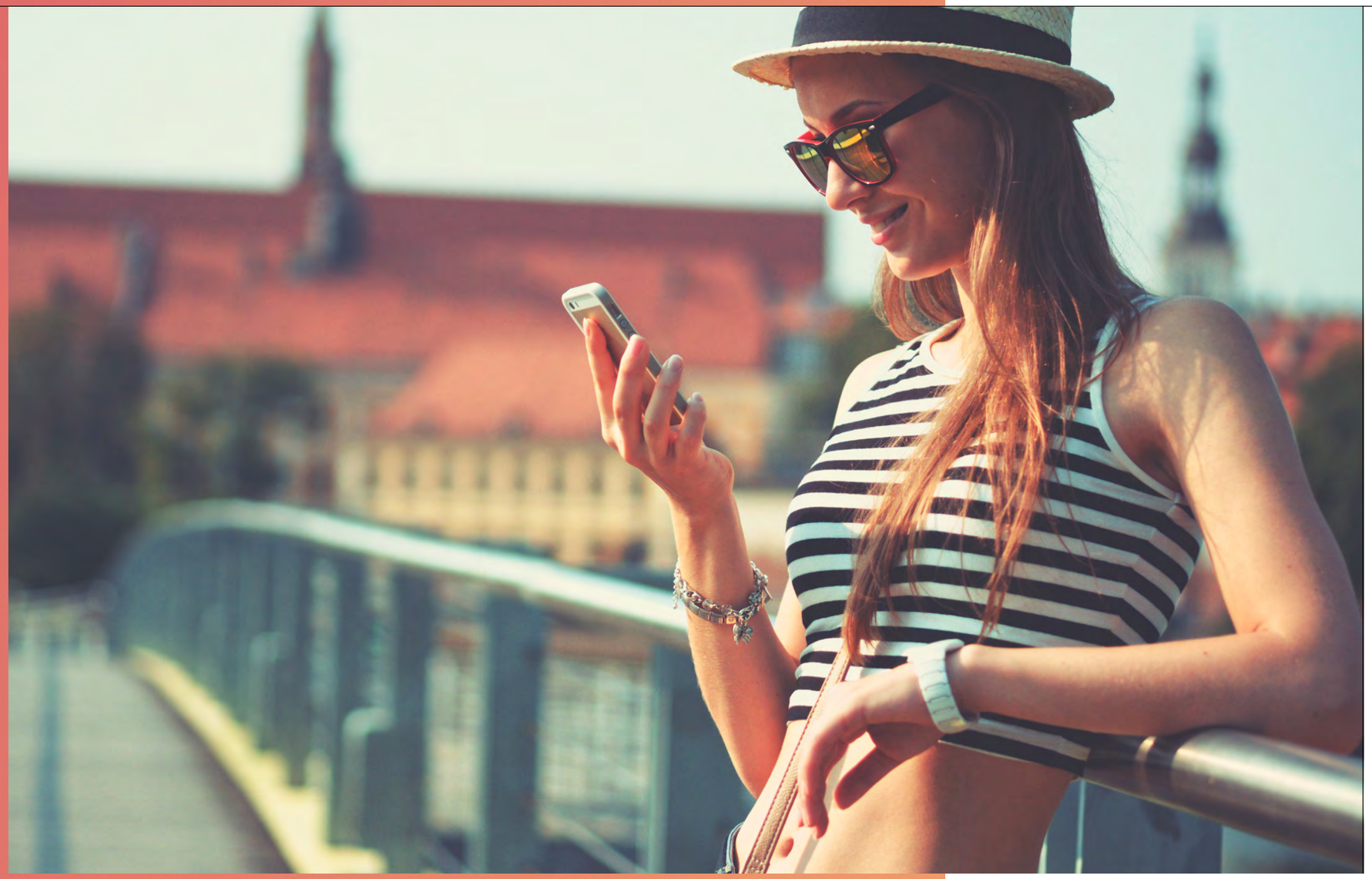
04

What regulatory reforms could reduce cyber risk?

How could law enforcement be better resourced?

How could consumer awareness and education reduce cyber risk in relation to piracy sites?

Discussion



The results of this study indicate a very high risk of encountering cyber threats while using digital piracy services in Poland. In the worst case, if a consumer visits the top 30 P2P piracy sites, they would be exposed to 77 cyber threats, with a relative risk of 38.50 compared to a set of mainstream controls.

By comparing the relative risk to a set of controls, we can determine the exact increase in cyber risk that can be assigned to visiting digital piracy sites against the baseline level of cyber risk inherent in visiting any website. Further blocking access to digital piracy sites, and doing so faster, would result in a material reduction in overall cyber risk in Poland at a time when it is already very high.

We make a number of policy recommendations that could be considered by Polish authorities to make further inroads in reducing cyber risk for consumers in Poland, noting that many of them are likely to be teen or pre-teen consumers. Based on the evidence presented in this report, the most significant reform would be introducing administrative site blocking to enable transparent and timely blocking of a small number of websites.

What regulatory reforms could reduce cyber risk?

With respect to cyber risks from digital piracy, Poland's legal framework includes the general possibility of applying for interim injunctions granted in the criminal or civil court procedures against a defaulted party, which may be applied also in the context of website blocking of copyright infringement. Website blocking orders as no-fault injunctions against an internet service provider as an innocent party are not addressed directly in Polish law.

The process of granting injunctions by the court can be very slow when compared to administrative site blocking. Given the urgency of "zero day" cyber threats, time is of the essence, and speedy but proportionate measures could therefore reduce the impact on consumers from further infection or exploitation.

A good example is the registry of gambling domains (https://hazard.mf.gov.pl/). Expanding this approach to include domains solely associated with piracy, and which ISPs could then block, could provide timely responses to cyber threats associated with digital piracy sites, while also providing transparency about blocking.

Other ways of reducing cyber risks in Poland, especially from digital piracy, involve a combination of regulatory reforms, collaborative efforts, and technological advancements.

Continuous refinement of national regulations to align with the requirements of the EU Directive on Security of Network and Information Systems (NIS) could help improve the overall cybersecurity posture.

Further national cybersecurity legislation that addresses emerging threats, establishes clear responsibilities, and defines measures for securing critical infrastructure and sensitive data, could also be considered. Mandatory data breach notification requirements for organizations could also be further developed, to encourage prompt reporting of security incidents, enabling faster response and mitigation efforts.

Further enforcing cybersecurity standards for critical infrastructure sectors and encouraging organizations to obtain cybersecurity certifications to demonstrate compliance with industry best practices, could also reduce sector-wide cyber risk. Organizations should also be encouraged to develop and regularly test incident response plans- this ensures preparedness and a swift response to cyber incidents.

Further regulation to address supply chain security, requiring organizations to assess and manage the cybersecurity risks associated with their suppliers and service providers. Organizations should be required to assess and monitor the cybersecurity practices of vendors and partners.

How could law enforcement be better resourced?

Ensuring law enforcement is well-resourced to deal with cyber threats arising from piracy sites in Poland involves a multi-faceted approach, combining legal, technological, and collaborative efforts. Further specialized cybercrime units within law enforcement agencies dedicated to addressing online piracy and related cyber threats could be established.

These units should be equipped with the necessary skills, training, and expertise in digital forensics, cybersecurity, and intellectual property rights enforcement. There is also a need to further invest in ongoing capacity building and training programs for law enforcement personnel, as cyber threats are dynamic. Providing continuous training on emerging trends, investigative techniques, and digital tools is crucial for effective response.

There is also a need to ensure law enforcement agencies have the necessary technological infrastructure to conduct digital investigations and respond to cyber threats. This includes tools for digital forensics, data analysis, and collaboration platforms. Enhanced capabilities for handling digital evidence will ensure it is admissible in court; training for law enforcement personnel on preserving and presenting digital evidence during legal proceedings is vital.

Strengthening support mechanisms for cybercrime victims and establishing user-friendly reporting mechanisms could also reduce the time taken to investigate and respond to cyber threats. Encouraging individuals and businesses to report incidents promptly and facilitating law enforcement's ability to take action should be considered. One possible innovation could be a one-click reporting tool for consumers to flag cyber threats on piracy sites as they are encountered, capturing vital digital evidence and preserving this forensic data for subsequent enforcement action. However, for these innovations to be effective, incident response and triage must be in place, and, as mentioned above, administrative site blocking is needed to swiftly block threats as they are identified.

By combining these strategies, Poland can better equip its law enforcement agencies to address cyber threats emanating from piracy sites.

How could consumer awareness and education reduce cyber risk in relation to piracy sites?

Consumer awareness and education are vital in reducing cyber risks related to piracy sites in Poland. By informing consumers about the potential dangers associated with engaging with piracy sites and promoting responsible online behavior, consumers (including the teen and pre-teen demographic) can make more informed decisions. An action plan could include the following tactics:

- Educate consumers about the various risks associated with piracy sites, such as exposure to malware, phishing attacks, and potential legal consequences. Highlight the dangers of downloading or streaming content from unauthorized sources.
- Emphasize the heightened risk of malware infections and other cyber threats on piracy sites. Consumers should be aware that these sites often host malicious software that can compromise the security of their devices and place them at risk of ransomware, identity theft, credit theft, spyware, and sextortion.
- Raise awareness about phishing tactics commonly employed by cybercriminals on piracy sites. Consumers should be cautious about providing personal information, such as login credentials or financial details, to suspicious websites.
- Educate consumers about the legal consequences of engaging with piracy sites. Unauthorized downloading or distribution of copyrighted content can lead to legal action, fines, or other penalties. Promote the use of legal and licensed platforms for content consumption.
- Provide guidance on safe online practices, including the importance of updating software and antivirus programs and the dangers associated with piracy sites and services. Encourage using legitimate streaming services and official content distribution platforms to reduce exposure to cyber threats.
- Integrate digital literacy programs into educational curricula and public awareness campaigns. Equip individuals with the skills and knowledge needed to navigate the digital landscape safely, identify potential threats, and make informed decisions.
- Launch public awareness campaigns to inform consumers about the risks associated with piracy sites. Use various channels, including social media, educational institutions, and government initiatives, to disseminate information and promote responsible online behavior.
- Collaborate with ISPs who can play a role in educating their subscribers about the risks involved.
- Integrate cybersecurity concepts into media literacy programs to help individuals critically assess the sources of online content and understand the potential risks associated with consuming content from unverified platforms.

Further protecting consumers using these strategies is consistent with the consumer education goal identified in the National Cybersecurity Strategy.

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 Adjunct Professor of Cybersecurity at La Trobe University and Honorary Professor of Security Studies and Criminology at Macquarie University.

Professor Watters is a Chartered IT Professional, a Fellow of the British Computer Society, a Senior Member of the IEEE, a Member of the ACM, and a Member of the Australian Psychological Society. His work has been cited 8,149 times, with a *h*-index of 41 and an *i*-10 index of 133.

He is in the top 10 percent of SSRN-cited authors globally.

Bibliography

05

Bibliography

Bibliography

1. https://www.trade.gov/market-intelligence/poland-ict-most-cyber-attacked-country-world
2. Chen, J., Gao, Y., & Ke, T. T. (2023). Regulating digital piracy consumption. Available at *SSRN 4198295*.
3. Deloitte (2023). Theft of video content on the internet: Analysis of the impact of online piracy of audiovisual content, including television content, on Poland's economy.
4. Watters, P.A. (2021). Consumer risk and digital piracy – where does malware come from? *Available at SSRN 4536938*.
5. Tomczyk, Ł. (2021). Evaluation of digital piracy by youths. *Future Internet*, 13(1), 11.
6. De Kosnik, A. (2020). Piracy is the future of culture: Speculating about media preservation after collapse. *Third Text*, 34(1), 62-70.
7. For a Polish study, see Tyrowicz, J., Krawczyk, M., & Hardy, W. (2020). Friends or foes? A meta-analysis of the relationship between "online piracy" and the sales of cultural goods. *Information Economics and Policy*, 53, 100879.
8. Başeskioğlu, M. Ö., & Tepecik, A. (2021). Cybersecurity, computer networks phishing, malware, ransomware, and social engineering anti-piracy reviews. In *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications* (HORA) (pp. 1-5). IEEE.
9. Iqbal, A., Aman, M. N., Rejendran, R., & Sikdar, B. (2024). Unveiling the Connection Between Malware and Pirated Software in Southeast Asian Countries: A Case Study. *IEEE Open Journal of the Computer Society.*
10. Watters, P. (2023). Consumer risks from piracy sites in the Philippines. Available at *SSRN 4536945*.
11. Lockett, A., Chalkias, I., Yucel, C., Henriksen-Bulmer, J., & Katos, V. (2023). Investigating IPTV Malware in the Wild. *Future Internet*, 15(10), 325.
12. Araucz-Boruc, A. (2021). Police in fight against organised crime—problem identification. *Przegląd Policyjny,* 140, 164-172.
13. Dalinczuk, L. (2020). Organized crime as a threat to national security. Doctrina. *Studia społeczno-polityczne*, (17).
14. https://www.trade.gov/market-intelligence/poland-ict-most-cyber-attacked-country-world
15. Choi, J., & LaPrade, J. (2023). Internet piracy. *Handbook on Crime and Technology*, 165-177.
16. McKenzie, J. (2020). Digital piracy. *Handbook of Cultural Economics*, Third Edition, 228-234.
17. Rajiv Shah, Deniz Cemiloglu, Cagatay Yucel et al. Is cyber hygiene a remedy to IPTV infringement? A study of online streaming behaviours and cybersecurity practices, 12 November 2023, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-3579394/v1].
18. 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/
19. Jennings, K., & Bossler, A. M. (2020). Digital piracy. *The Palgrave handbook of international cybercrime and cyberdeviance*, 1025-1045.
20. Czetwertyński, S. (2023). Digital piracy: the issue of knowledge of the institution of copyright law. Ekonomia i Prawo. *Economics and Law*, 22(1 (Forthcoming)).
21. https://www.imf.org/external/datamapper/profile/POL
22. Noting that increasing citizen awareness is a key pillar in the national cybersecurity strategy (https://www.cyberwiser.eu/poland-pl).
23. Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 4(1), tyy004.
24. Riek, M., Böhme, R., Ciere, M., Ganan, C., & van Eeten, M. (2016). Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries. In *Workshop on the Economics of Information Security (WEIS), University of California at Berkeley* (Vol. 2).
25. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new
26. Kitler, W. (2022). The Cybersecurity Strategy of the Republic of Poland. *Cybersecurity in Poland*, 137.
27. https://archiwum-ncbc.wp.mil.pl/en/index.html
28. https://csirt.gov.pl/cee
29. Szpor, G. (2021). The evolution of cybersecurity regulation in the European Union law and its implementation in Poland. *Rev. Eur. & Comp*. L., 46, 219.
30. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework
31. https://www.enisa.europa.eu/
32. https://ik.org.pl/en/2024/01/30/establishment-of-the-tallinn-mechanism-polish-support-for-ukraines-cybersecurity/
33. https://www.saferinternet.pl/menu/about-us/safer-internet-in-poland.html?setlng=en
34. 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 55 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. For more information, visit www.alliance4creativity.com
35. For more details of how VirusTotal works, see https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works
36. Note that any potential false positives have neither been identified nor excluded from the results, as the researchers do not have access to the raw results from each security vendor.

Acknowledgements

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

Appendices

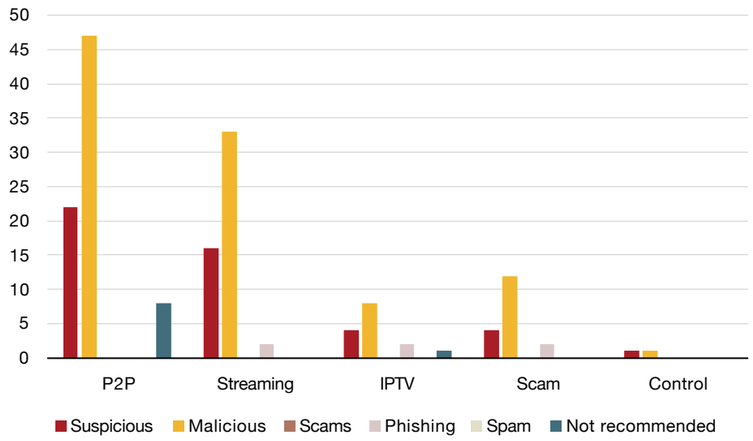
06

Appendix A
Appendix B

Appendix A

Cyber threat category results—Worst-case scenario

	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
P2P	22	47	0	0	0	8
Streaming	16	33	0	2	0	0
IPTV	4	8	0	2	0	1
Scam	4	12	0	2	0	0
Control	1	1	0	0	0	0



Appendix B

Cyber threat category results—Best-case scenario

	Suspicious	Malicious	Scams	Phishing	Spam	Not Recommended
P2P	17	24	0	0	0	7
Streaming	11	16	0	1	0	0
IPTV	4	8	0	2	0	1
Scam	4	7	0	1	0	1
Control	1	1	0	0	0	0