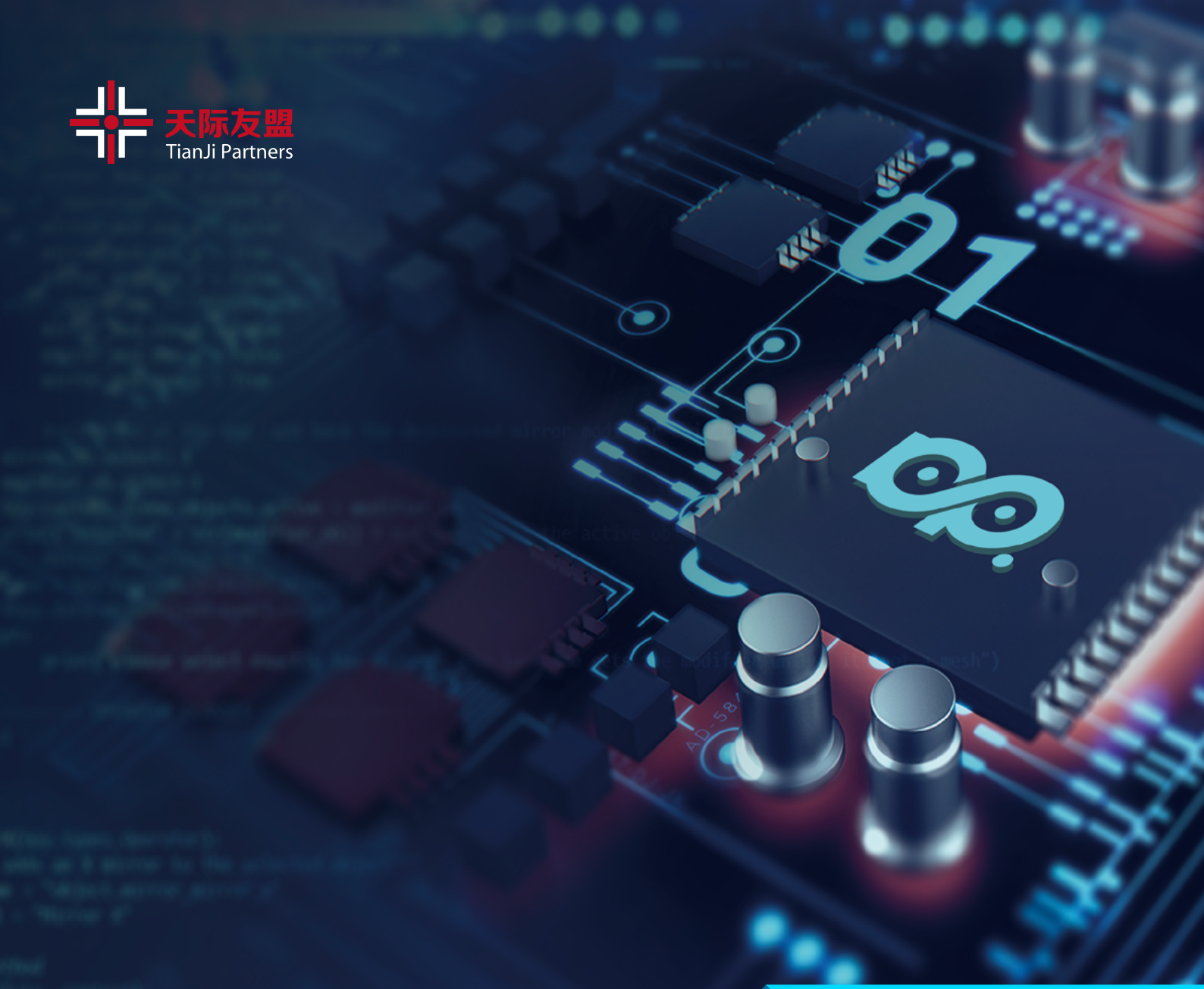
天际友盟
TianJi Partners



China
Digital Risk Protection Report
(2021)

2022-02

Gemini Lab

Preface

In 2021, the Covid-19 pandemic has become a double-edged sword. While seriously affecting people's daily lives, it has also accelerated the pace of the global digital economy. Enterprises are increasingly relying on online channels to improve daily productivity, customer engagement and business growth. Because of this reliance, businesses need to protect these channels from risks such as phishing, brand infringement, data breaches, etc. Digital Risk Protection's mission is to protect modern businesses from all forms of external digital threats.

Dealing with digital risks properly during business transformation allows enterprises to make full use of digital transformation technologies and truly enjoy the benefits brought by it. More and more enterprises have recognized the importance of protecting their brands, personnel and data, which will be a driving force of acquiring their competitive advantages in the market.

However, it is found that risk management teams struggle to handle with the explosive growth of digital assets. They are tasked with digital risks surpassing the capabilities of individual teams in both coverage and complexity. Digital risk solutions driven by modern technologies are dedicated to helping enterprises develop appropriate coping strategies when obstacles appear.

In July 2021, Tianji Partners, with rich experience in the field of digital risk protection, released the first "China Digital Risk Protection Report" . The report systematically sorts out the Chinese domestic digital risk situation in the first half of 2021, and providing business executives in various industries with concept of digital risk management and risk data required for quick response and decision-making.

Digital risks bring a variety of changes in speed and magnitude as time flies. In order to further help enterprises improve the awareness of digital assets protection and better resist external threats, Tianji Partners has conducted a complete digital risk analysis for 2021, expecting that it can be a reference for modern enterprises to deal with digital risks.

Digital
Risk Protection

contents

01 Overview of Digital Risk Protection

1.1 Digital Risk Background

In 2021, the Covid-19 pandemic has become a double-edged sword. While seriously affecting people's daily lives, it has also accelerated the pace of the global digital economy and intensified government urgency to respond to this process. According to statistics from the "Global Digital Economy White Paper" released by China Academy of Information and Communications Technology (CAICT), the added value in 2020 of the digital economy in 47 countries will reach 32.6 trillion US dollars, a nominal increase of 3.0% year-on-year, accounting for 43.7% of GDP. And, China's digital economy developed by leaps and bounds. Tot only the growth rate became the first in the world, but the market size broke through again and again. It was close to the scale of 5.4 trillion US dollars, ranking second in the world. The proportion of the core industries of the digital economy in Chinese national GDP has also continued to increase. Through digital innovation, Chinese companies have the opportunity to become a key force in changing the global competitive landscape in the future. It can be seen that digital innovation has become the top priority for economic development in China and even across the world.

The Party Central Committee has been attaching great importance to the digital economy development. General Secretary Xi Jinping pointed out that since the 18th National Congress of the Communist Party of China, the CPC Central Committee has implemented the strategy of country strengthening through Internet and the national strategy of big data, prospering Internet economy, promoting the deep integration of the Internet, big data, artificial intelligence and the real economy, and building the digital China, the intelligent society, and promoting digital industrialization and industrial digitization. In this context, Chinese digital economy has developed rapidly and achieved remarkable achievements. Especially since the outbreak of the pandemic, digital technologies such as live streaming, online medical treatment, online education, and online office have played an important role in supporting the fight in restoring production and life against the pandemic.

The continuous maturity of digital technology is accompanied by various digital risks. It is estimated that in 2022 global internet traffic will exceed the sum of internet traffic as of 2016. With such a huge volume and no geographical boundaries, the cyberspace is bound to be chaotic and the management process will be difficult. Digital threats such as phishing, brand infringement, social media phishing, ransomware, and data breaches are harming businesses and netizens in countless ways. When coming across various risks, due

to the lack of sufficient advanced preparation and effective risk protection measures, enterprises usually delay the best time to solve the problem, which not only causes irreversible public opinion pressure on their own brands, but also triggers serious direct economic losses to consumers. In response to this situation, Gartner recommends that organizations should establish a new "digital trust and security" team, focusing on maintaining healthy interactions between consumers and brands, while seeking threat emergency support from professional service teams to ensure the healthy and continuous communication between enterprises and consumers to ultimately realize the brand value. The establishment of internal and external protection mechanisms is a necessary choice for enterprise digital assets protection.

1.2 Regulatory compliance

With the increasingly close connection between the Internet and people's daily life, network information management is also imminent. National leaders attach great importance to the legitimate rights and interests of citizens, legal persons and other organizations. In recent years, in order to create a good network ecology, China has successively issued a series of laws and regulations such as the "Cyber Security Law", "Regulations on the Ecological Governance of Network Information Content" and "Measures for the Administration of Internet Information Services", dedicated to safeguarding national security and public interests , building a network environment with clear weather.

Furthermore, for better implementation, relevant national departments have further intensified supervision and put forward rectification requirements for some leading Internet companies regarding Internet information security problems. Recently, the Network Security Administration of the Ministry of Industry and Information Technology and the Criminal Investigation Bureau of the Ministry of Public Security jointly interviewed the relevant persons in charge of Alibaba Cloud and Baidu Cloud, and reported the number of fraudulent websites to which the two companies have accessed fraudulently in their efforts to prevent and control telephone scam and network fraud. If the problems remain high, it is required to earnestly fulfill the main responsibility of network and information security entity and rectify the relevant problems within a time limit. Those who refuse to rectify or the rectification will be severely punished in accordance with laws and regulations. Both companies expressed that they would earnestly implement the regulatory requirements, further strengthening the management of website access, domain name registration, information services, etc., and effectively preventing the risk of telecommunication network fraud.

The listing in the US stock market of a Chinese corporation in 2021 brought the issue of APP's acquisition of user data to the forefront. In the same year, CNCERT and the Cyber Security Association jointly established a platform for monitoring the collection and misuse of personal information by apps, and a platform for accepting apps reports, summarizing and sorting out the problems of illegal collection and misuse of personal information by apps. According to the statistics, several well-known app stores with controversial privacy problem are Liqu App Market, Xixi Software Park, and Green Resource Network.

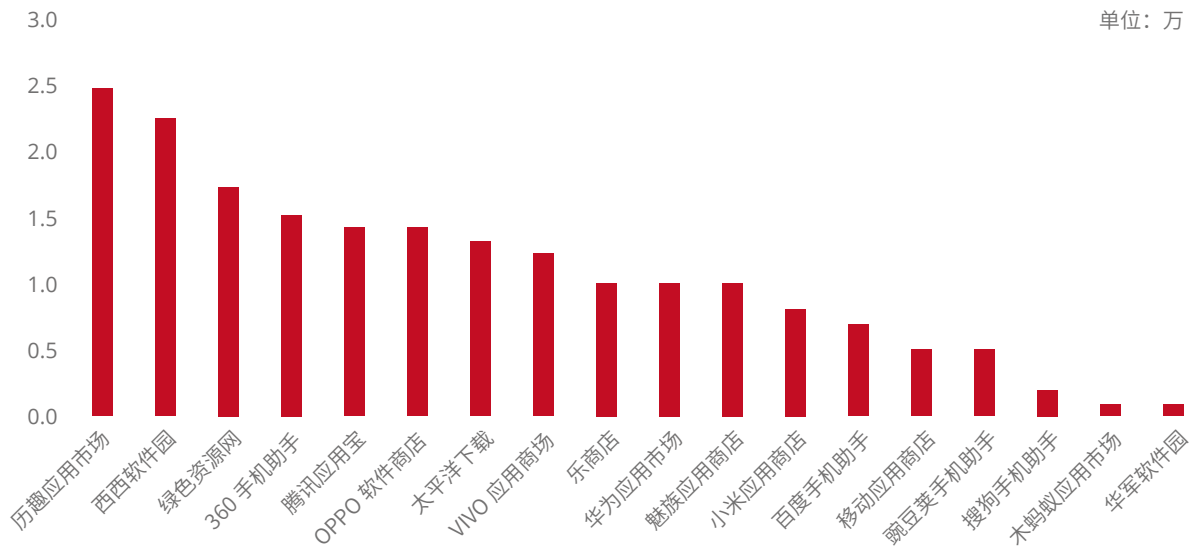


Figure 1: Distribution of issues concerning the collection of personal information by mainstream app stores before the privacy policy

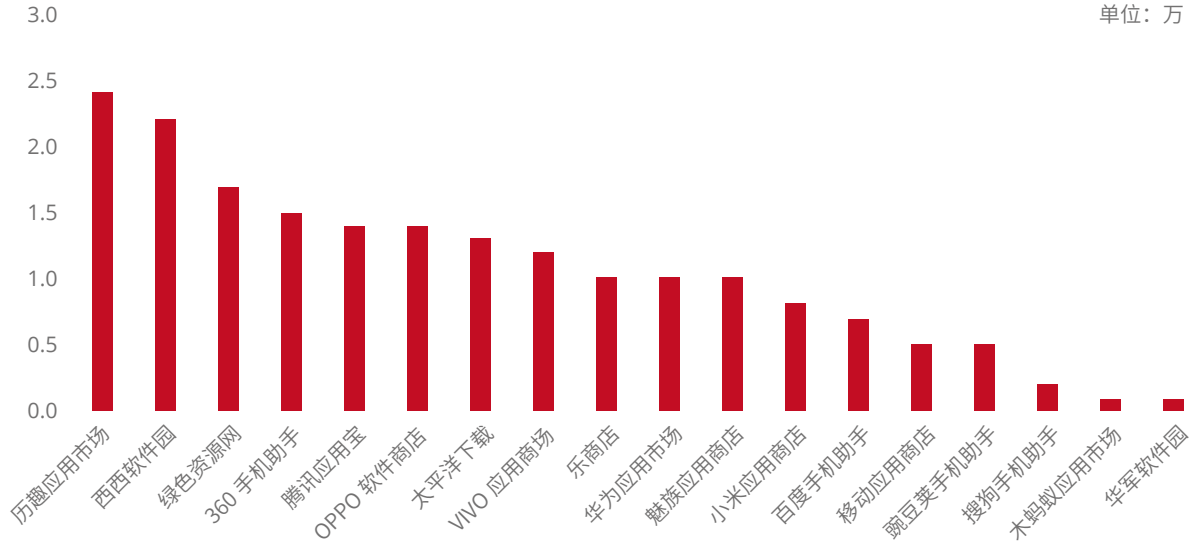


Figure 2: Distribution of issues related to pop-up windows in mainstream app stores asking for irrelevant permissions

Strengthening the supervision of digital service providers, maintaining the national Internet order, and protecting the rights and interests of netizens are the core responsibility of Internet law enforcement agencies around the world. Aleksandr Grichishkin, the Russian founder of a hosting company, has been sentenced to 60 months in prison for allowing a cybercriminal group to use his platform to attack U.S. financial institutions between 2008 and 2015. During the operations, he provided the infrastructure (including IP addresses, servers, and domain names) needed to distribute malware, host phishing kits, target networks break in, botnets building, and stealing bank login information for a number of cyber criminal campaigns. The Federal Deposit Insurance Corporation (FDIC) estimates that the SpyEye and Zeus attacks alone cost banks and their corporate customers approximately $64 million in 2011.

It can be seen that the supervision of network service providers is of great significance to national Internet governance.

1.3 Scope of Digital Risk Monitoring 2021

In 2021, Tianji Partners conducted digital risk monitoring on a total of 3,146 brands domestic and abroad. The brands involve more than ten industries such as finance, Internet, government, large enterprises, education, copyright piracy, media, medical care, real estate, industrial manufacturing, and international trade, etc.

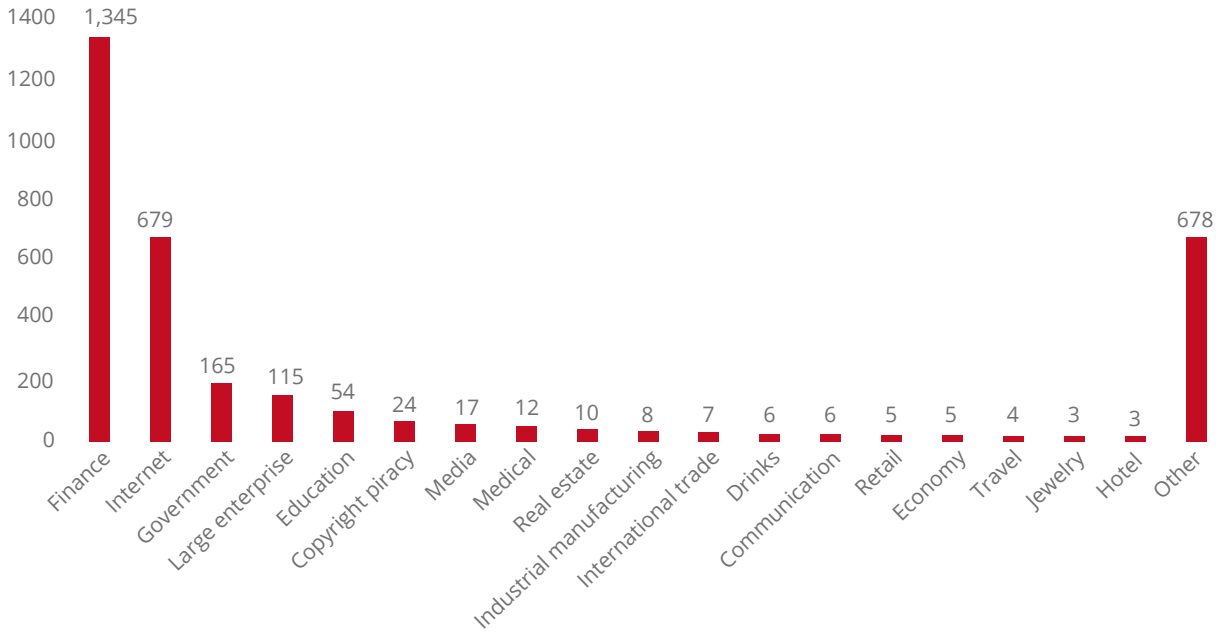


Figure 3: industry distribution of monitored brands

Industry	Quantity
Finance	1,345
Internet	679
Government	165
Large enterprise	115
Education	54
Copyright piracy	24
Media	17
Medical and health care	12
Real estate	10
Industrial manufacturing	8
International trade	7
Drinks	6
Communication	6
Retail	5

Economy	5
Travel	4
Jewelry	3
Hotel	3
Other	678
Total	3,146

Table 1: industry distribution of monitored brands

1.4 Executive Summary

Phishing fraud

Total digital risk NO.1

The number of phishing scams remains "one-of-a-kind" ahead of other digital risks due to the direct benefits of phishing scams. In a certain period of time, phishing fraud will remain the focus of digital risk prevention.

Data breaches

Digital risk growth NO.1

As one of the key points C (confidentiality) of the information security CIA (confidentiality, integrity, availability) , the loss of network security brings about the "double-kill" dilemma of data. One is encryption and blackmail, and the other is derivative risks triggered by data leakage. Data breaches will undoubtedly constitute a large proportion of digital risks and continue to grow rapidly.

Financial industry

Digital risk industry NO.1

The financial industry has always been the hardest hit area for digital risks due to the characteristics of the industry, namely risk management, which is directly linked to currencies. It is foreseeable that the financial industry, as a high-incidence area of digital risks, will remain unchanged for a long time.

Internet Service Provider NO.1

Alibaba Cloud
21.72%

Domain Name Service Provider NO.1

GoDaddy
16.76%

Country NO.1

United States
34.65 %

Social media platform NO.1

Weibo
39.85 %

APP store NO.1

Liqu
10.4 %

The key development trends of digital risk are as follows:

Centralization of service providers:

Some cloud service providers indirectly become the biggest accomplice of lawbreakers for no effective regulatory managements. Therefore, the cloud has also become a hiding place for digital risks.

Diversification of use case:

Various methods that can realize direct or indirect benefits have led to the development of many new use cases of digital risks.

Location overseas:

Risks are distributed globally for areas with law system less strict.

02 Digital Risks Assessment Model

With the digital transformation of enterprises, digital risk management theory is gradually recognized by enterprise managers on the basis of information risk management. In order to study digital risks thoroughly, the concept of FAIR model is introduced here. The FAIR model is a widely used in cybersecurity risk assessment (CRA) framework in the field of information security.

The FAIR (Factor Analysis of Information Risk) model is generated to mitigate and prevent the intractable network security questions that have appeared in the network environment developing with exponentially increasing complexity due to that a large number of enterprises rely on the rapid development of information technology. These problems occur and exist in countless forms such as data leakage, brand infringement which damage corporate reputation and ultimately cause direct and indirect financial losses to corporations. The FAIR model assesses cyber security risks, helping risk managers prioritize digital risks, allocating limited resources to mitigate digital risks, and making further preventive decisions.

2.1 FAIR Model

The FAIR model uses a taxonomy to interpret risk (financial loss) into risk factors, taking into account the competency competition between attackers and defenders, as well as the vulnerability of information assets, attack frequency, and financial loss to measure a risk. The FAIR model describes the relationship between risk factors as follows. (See below):

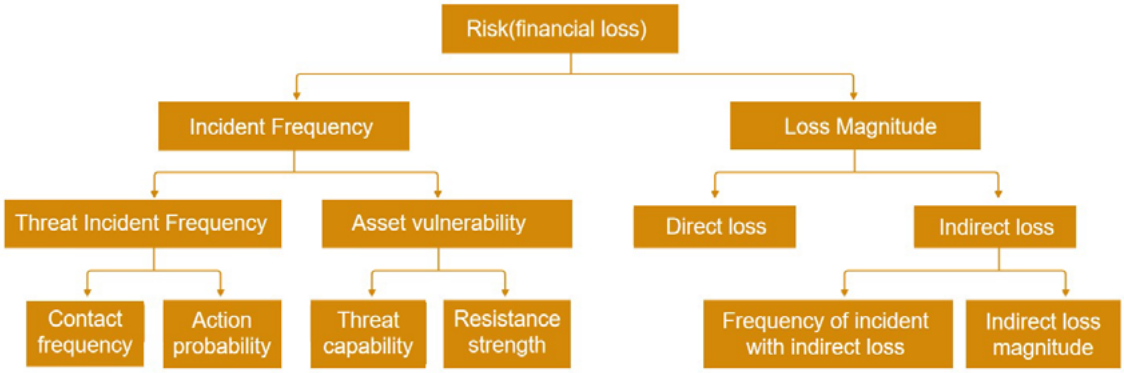


Figure 4: FAIR Model

The FAIR model models risk categories. In risk classification, risk factors need to be exhaustive and mutually exclusive. The overall risk (financial loss) is described by the product of the events frequency and the loss magnitude. That is: risk (financial loss) = incident frequency * loss magnitude.

Incident frequency refers to the frequency with which attackers cause damage to information assets within a given time, expressed by the product of threat incident frequency and asset vulnerability (incident frequency = threat frequency frequency * asset vulnerability), where the former means " The frequency with which an attacker takes action against an information asset", the latter is defined that "the likelihood that an information asset will not be resistant to an attacker's action".

Threat incident frequency is the frequency of contact between the attacker and the asset, and the probability (action probability) that the attacker will take action on the asset once it contacts the target information asset (contact frequency), expressed as threat incident frequency = contact frequency * action probability.

Asset vulnerability is the difference between the level of force that a threat factor can exert on an asset (threat capability) and the defender's strength of control over the asset (resistance strength), expressed as asset vulnerability = threat capability - resistance strength.

The loss magnitude is composed of direct loss and indirect loss, which is indicated as loss magnitude = direct loss + indirect loss. In the FAIR model, indirect loss is called secondary loss. Typical examples include negative impact on corporate brands and increased capital costs.

The indirect loss can be interpreted as the frequency of indirect loss events and the magnitude of indirect loss, expressed as: indirect loss = frequency of events with indirect loss * indirect loss magnitude.

In summary, the complete risk formula of the FAIR model is demonstrated as: risk = (contact frequency * action probability) * (threat capability - resistance strength) * (direct loss + frequency of events with indirect loss * indirect loss magnitude).

2.2 Digital Risk Analysis Model (C-FADR Model)

In some specific circumstances of digital risk, the FAIR model has certain constraints.

Openness of information assets: In the field of digital risk research, the main targets of attacks are publicly released application systems, including: corporate websites, mobile applications, corporate official accounts and senior management official accounts, which are typically available. The concept of data leakage mentioned in digital risk protection is also based on the premise that digital information has been leaked.

Availability of attack capabilities: Due to the promotion of open source testing software, various testing software and learning materials are extremely easy to obtain. However, these software are double-sided, which can be used for testing and improvement of application systems, and also used by attackers. Due to the publicity of assets, attacks on websites, apps, public account, etc. basically have great chance of success against little resistance.

Threat event measurability: Digital risk attacks are necessary to be publicly released to have an attacking effect. Continuous monitoring on the Internet, mobile Internet, deep web and dark web are executed to perceive threat events , and statistical principles to calculate and evaluate the frequency of threat events. Therefore, threat events are measurable, the measurement process controllable, and the measurement results credible.

Based on the above constraints, the FAIR model of digital risk can be simplified as the following figure:

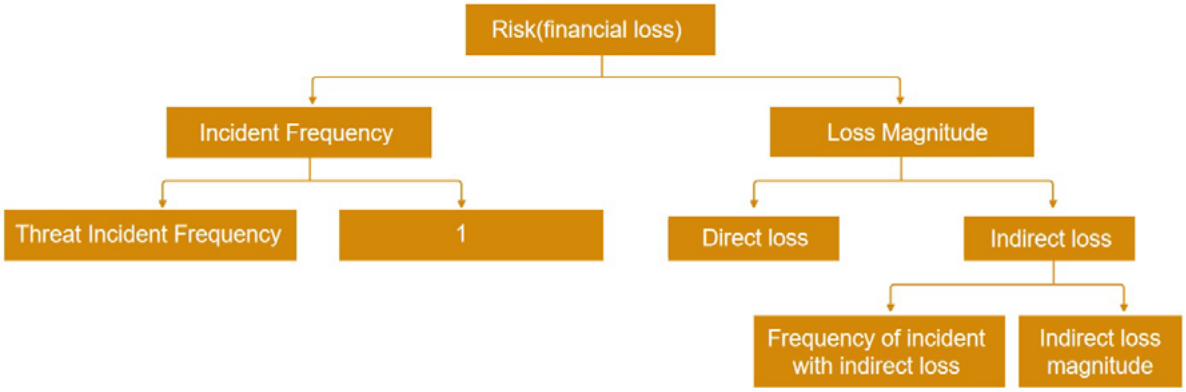


Figure 5: Digital Risk FAIR Model

Since the premise of the above model is the constraint assumption for the measurement of threat incident and asset vulnerability, the model is defined as constraint-Factor Analysis of Digital Risk, or C-FADR for short. Expressed as:

risk = threat incident frequency * (direct loss + frequency of incident with indirect loss * indirect loss magnitude).

The simplified digital risk formula is easier to apply, and businesses can quickly complete risk assessments by monitoring Internet threats and gathering information from internal investigations.

2.3 Loss Magnitude Analysis

2.3.1 Defender View

In risk models, it is always difficult to count losses, especially when losses consist of direct and indirect losses. If indirect losses are like the hidden part of an iceberg underwater, it is more difficult to estimate. However, through scientific estimation models, indirect losses can still be calculated, and even rough estimates can be made using empirical formulas, just like the overall volume of the iceberg calculated by the density rate on the basis of the part of the iceberg floating on the water.

For the scope of research on digital risk, the direct loss will be in a smaller proportion. The direct loss here refers to the monetized loss directly suffered by the enterprise after the incident occurs. And the amount of the loss can be quantified before the loss. The primary loss of digital risk includes indirect loss. Indirect loss refers to the loss that may occur after the event occurs, the probability of which is greater than 0 and less than 1, and with a certain probability. It may include:

~Civil, criminal or contract fines and sentences

~ Notification fee

~Credit Monitoring

~ Make up for lost money to secondary stakeholders

~Public relations expenses

~ Legal defense fees

~Disposal costs, which consist of the salaries of front-line personnel, public relations, legal affairs, and other related personnel

*Impact of regulatory sanctions

* Lost market share

*Shares fall

*Increased cost of capital

For the above indirect costs, for subjects with a ~ symbol, corporations can obtain relatively accurate figures through research, with errors controllable. For the subjects marked with *, the features of the long-term nature, importance, and increasing inaccuracy taken into account, corresponding costs need to be invested to obtain more accurate figures.

2.3.2 Attacker View

In the previous section, the report adopts a defender's perspective to analyze digital risk, which is also a commonly used analytical perspective in risk models. However, in some use cases, analysis only out of the perspective of defenders is not comprehensive. For example, the losses caused by phishing government websites often cannot be simply measured by the monetization losses, direct and indirect. At this time, it is necessary to introduce the attacker's perspective. It is often said that A man's wealth is his own ruin by causing other's greed. Adopting an attacker lens can make businesses and organizations pay more attention to their social responsibility.

Since attacks on digital assets result in directly or indirectly monetary outcome, and the characteristics of low technical requirements, low crime cost, and hiding from law, analyzing attackers can obtain valuable intelligence information, which makes this model a primary analytical reference or business entities. In this premise, the digital risk model can be interpreted as:

Figure 6: Specific digital risk models

The formula is risk = threat incident frequency * attacker benefit. Among them, the attacker's benefit can be analyzed through public information.

2.4 Significance of Digital Risk Management

Digital risks are risks at scale that arise rapidly as digital transformation develops. The simplified and contextualized digital risk model can help enterprises and organizations cope with the challenges of digital risk modeling, redefining the priority matrix of information technology risks, and managing resources to deal with digital risks centrally and efficiently.

In addition to building digital risk models, businesses and organizations also need to take the responsibilities of digital risk management. Under the risk management framework, departments such as technology, risk control, legal affairs, and marketing need to perform their respective functions and cooperate with multiple parties under the unified leadership of the Digital Risk Officer (DRO), in order to cope with various risks with ease.

03 2021 Digital Risk Landscape in China

3.1 By Use Case

Common use cases can be divided into four categories: phishing fraud, data leakage, brand abuse, and false positive. The risk statistics for 2021 are as follows:

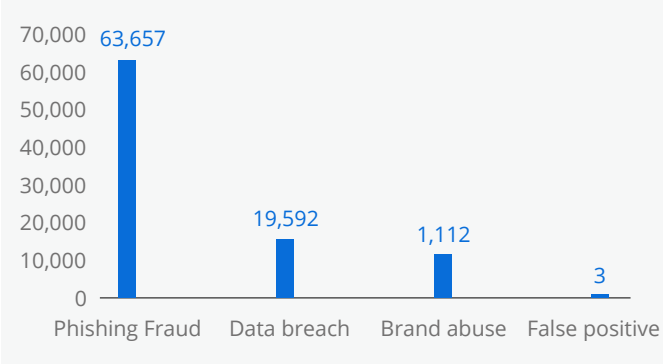


Figure 7: digital risk statistics by use cases in 2021

Use case	Quantity
Phishing Fraud	63,657
Data breach	19,592
Brand abuse	1,112
False positive	3
Total	84,364

Table 2: digital risk statistics by use cases in 2021

3.2 By Digital Asset

Common IT assets that are exposed to digital risks include websites, corporate data, mobile apps, copyrighted works, social media accounts, corporation codes, and emails. The risk statistics for 2021 are as follows:

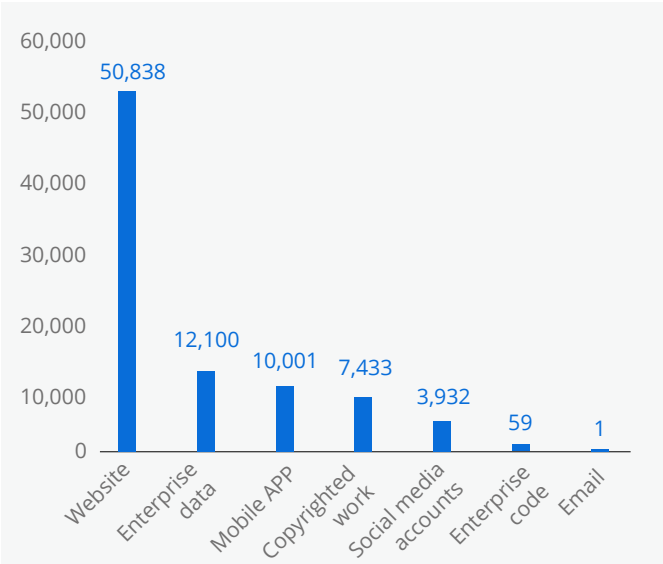


Figure 8: digital risk statistics by assets in 2021

Asset type	Quantity
Website	50,838
Enterprise data	12,100
Mobile APP	10,001
Copyrighted work	7,433
Social media accounts	3,932
Enterprise code	59
Email	1
total	84,364

Table 3: digital risk statistics by assets in 2021

3.3 By Industry

All industries are in the process of digital transformation. Certain digital risks distribute on different industries due to business forms and development stages, and continuing to vary and evolve. According to statistics, the digital risk distribution in industries in 2021 is as follows:

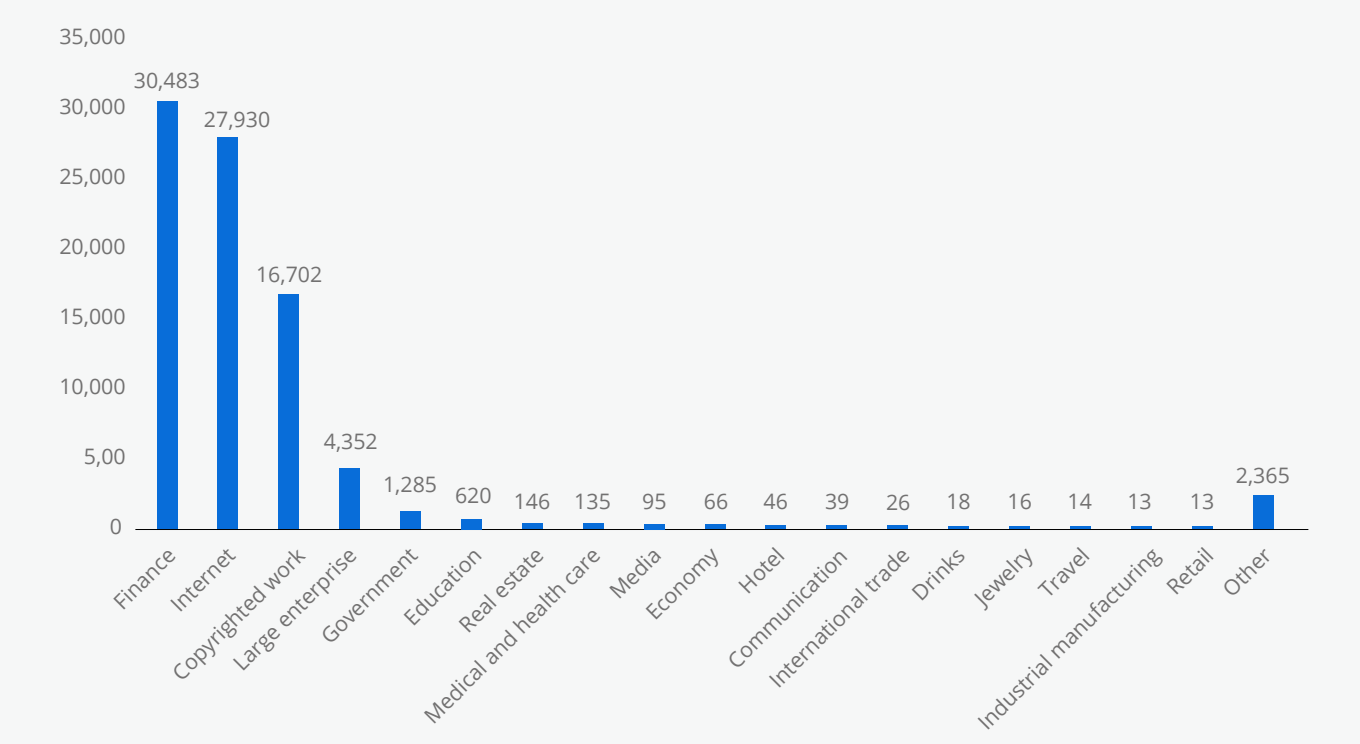


Figure 9: digital risk statistics by industry in 2021

Industry	Quantity
Finance	30,483
Internet	27,930
Copyrighted work	16,702
Large enterprise	4,352
Government	1,285
Education	620
Real estate	146
Medical and health care	135
Media	95
Economy	66
Hotel	46
Communication	39
International trade	26

Drinks	18
Jewelry	16
Travel	14
Industrial manufacturing	13
Retail	13
Other	2,365
Total	84,364

Table 4: digital risk statistics by industry in 2021

The financial industry can be subdivided into the following sub-sectors.

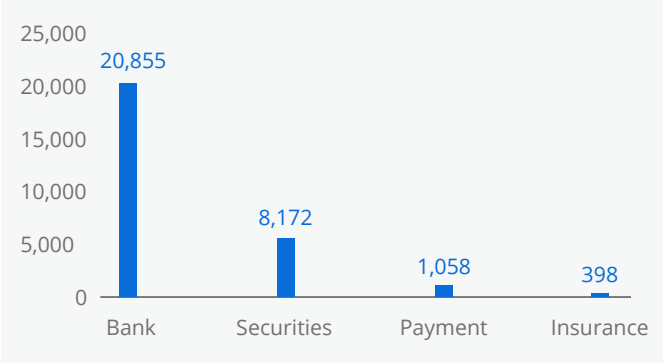


Figure 10: statistics of financial industry in 2021

Financial industry	Quantity
Bank	20,855
Securities	8,172
Payment	1,058
Insurance	398
Total	30,483

Table 5: statistics of financial industry in 2021

The Internet industry can also be further subdivided into the following sub-industries:

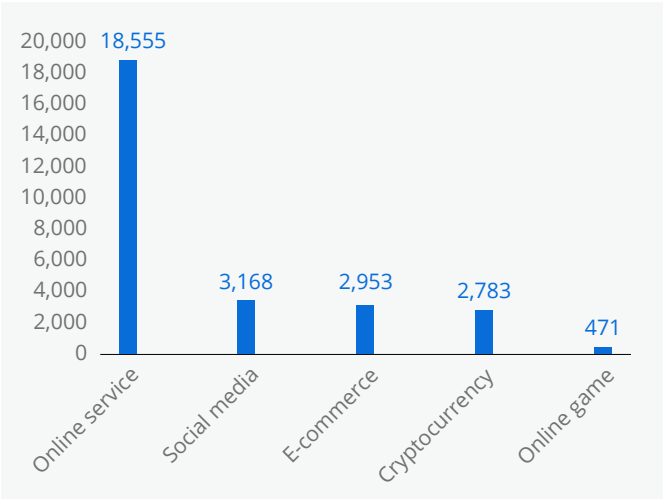


Figure 11: statistics of the Internet Industry in 2021

Internet industry	Quantity
Online service	18,555
Social media	3,168
E-commerce	2,953
Cryptocurrency	2,783
Online game	471
Total	27,930

Table 6: statistics of the Internet Industry in 2021

04 Digital Risk Deep Dive

4.1 By Tactics, Techniques and Procedures(TTPs)

4.1.1 Phishing for Banking Credentials

Phishing websites are contributed to stealing user's online bank login information. After account name and password obtained, attackers usually initiate an application for a new card, claiming the previous one stolen. Once the new card is ready to use, attackers transfer the balance left on the account immediately or swipe the credit card.

Figure 12: a phishing website impersonating a bank

4.1.2 Phishing for Personal ID Information

Personal identity theft is common in loan scams that have become frequent in recent years. For example, identity information stolen to apply for online loans, then attacker often make fraudulent calls to fool the victim who finally “returns” the loan to the attacker .

Figure 13: a phishing platform stealing personal information

4.1.3 Phishing for Organization Credentials

Phishing for enterprise authentication information mainly targets enterprises. Attackers use clone websites of government agencies such as the police, prosecution and law department to acquire important information of enterprises for various illegal activities , for instance, enterprise identity authentication, account opening under false names, and illegal loans.

Figure 14: a phishing website that steals corporate information

4.1.4 Unauthorized APP Distribution

Usually, the official APP of an enterprise will only be released to several mainstream official mobile application stores, such as the Apple Store, Huawei App Store, etc. However, due to the large number of third-party stores in the Android ecosystem, many store operators publish famous official APPs to their stores without authorization in order to attract more attention. This kind of behavior will bring a lot of security risks to the corporate brand. Moreover, if the third-party store is attacked, the official APP will face the possibility of being replaced with a malicious APP at any time.

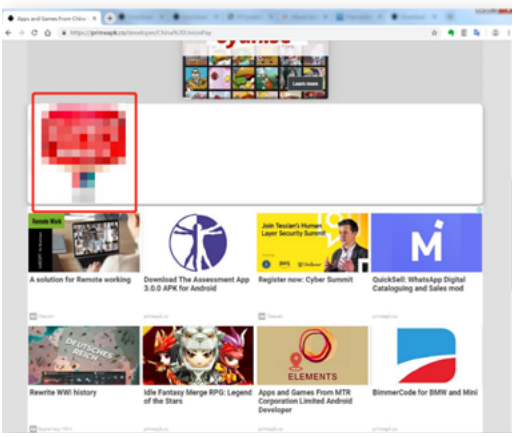


Figure 15: an unauthorized APP

4.1.5 Malicious Credential Stealing APP

Attackers often maliciously tamper with and repackage the official APP with reputation, and then use phishing websites or stores with little fame to spread mobile phone viruses or conduct fraud. Such malicious apps sometimes have no resemblance to official apps, but only misappropriate the brand's logo on the website page.

Figure 16: a malicious APP

4.1.6 Digital Brand Abuse

There are various ways to ride the wave of well-known brands, such as claiming to be an authorized partner to improve credibility, or to increase brand exposure through malicious rankings in search engines. And the code of the trusted website is inserted into the source codes of illegal gambling and pornographic websites to attract attention and avoid regulatory authorities' detection. Attackers can also package phishing and fraudulent pages as pages related to a well-known brand, tricking visitors into entering sensitive identity information and bank card information.

Figure 17: illegal gambling website impersonating a bank website

Figure 18: a counterfeiting coupons-giving food delivery website to steal ID information

4.1.7 Data Breach

Internal files and data are uploaded or even sold to code and document sharing platforms by former employees, suppliers or employees. Some breaches are the inadvertent actions of employees for the convenience of their work, while others are malicious acts, all of which are different manifestations of data breach risk. Even without malicious attention, the leakage has actually caused the result that confidential or sensitive documents can be accessed on the public network and bring certain risks to the enterprise.

Figure 19: An airline quarterly report is sold

4.1.8 Email Fraud

Commercial email fraud has always been a mainstream of malicious fraud over the world. Fraudsters use social engineering techniques to conduct phishing and fraudulent activities by registering domain names that are close to customer's and sending relevant emails. Different from pure email spoofing (Email spoofing forging email headers and spreading phishing URL links or malicious attachments), this type of email fraud is often more subtle, and the target is usually staff from company management or core departments such as finance. The fraud target and intention are also more obvious with greater harm to the business.

Figure 20: a phishing email

4.1.9 Film and Television Copyright Piracy

Copyright is the identity of digital works in the new era, but piracy has not stopped despite repeated prohibition. The attackers directly steal the author's achievements and damage the healthy development ecology of the industry. Cultural copyright works such as movies, novels, comics, variety shows, etc., have been pirated and leaked and played on various online websites, which seriously ruins the reputation and commercial value of copyright.

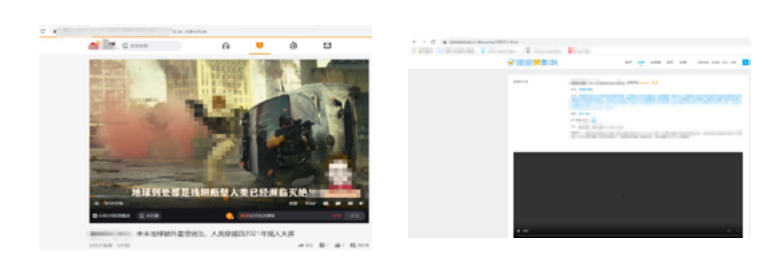


Figure 21: Pirated resources for a Hollywood movie in 2021

In addition to traditional film and television cultural works, sports live broadcast and other competition live broadcast, such as NBA, World Cup, UFC, e-sports, racing, etc.) have been pirated by hotlinks all year round, which also seriously destroys the healthy development of the live broadcast industry.

Figure 22: a pirated sport live streaming website

4.1.10 Copyright Infringement

Knowledge payment has been on the rise for a long time, along with its piracy industry chain. The main business interaction of knowledge payment is completely realized by the Internet platform, fraud and losses also mostly occur online. A large number of criminals illegally obtain paid intellectual assets from formal platforms through high-end technical means, they sell them at low prices through other channels. Many audience were lured by favorable prices and bought pirated resources. This not only causes direct economic losses to copyright institutions or copyright owners, but also is not conducive to building a positive brand image of knowledge platforms.

Figure 23: a well-known beauty academy's paid courses being pirated

4.1.11 Social Media Brand Abuse

In recent years, social media has become more than a communication tool to share opinions, insights, experiences and viewpoints with each other. More and more companies are also using the power of social media to actively shape the positive enterprise image, build up their brands, seek closer touch points with the consumers. The netizen also rely heavily on social media platforms to obtain current information. However, for the official nature of the object, most netizens do not have the ability to distinguish. A large number of attackers create fake accounts, and pretend to be employees or authorized service agencies on social media, trying to gain people's trust, and defraud various victim users of bank card, identity ID, passwords and other private information.

Figure 24: a fake customer service

4.1.12 Celebrity and VIP Impersonation

The personal image of a celebrity or corporate executive is the most valuable personal intangible brand asset and is closely related to the corporate brand image. When encountering risks, it will also bring business losses. Fake celebrity accounts existing on social media platforms will take advantage of public trust to spread false news or fraudulent information, which not only damages personal reputation, but may also cause public incidents and further business losses to enterprises.

Figure 25: fake celebrity accounts

4.1.13 Code Leakage

The popularization and application of the Internet has significantly improved office efficiency and has become an indispensable part of enterprise development. However, while the Internet brings convenience, it also faces external threats. The source code of the internal system often contains the

configuration file of the enterprise system, and even sensitive information such as passwords. If it is leaked to a third-party code open platform, the attacker can further analyze the logic loopholes of the code, or use it for phishing fraud. The risk of a company being attacked and compromised is greatly increased.

Figure 26: code leakage of enterprise intranet

4.2 By Threat Actors

4.2.1Financial Fraud Groups

The main purpose of financial fraud groups is to steal the login information, bank card of online services such as online bank, securities funds, and the personal information of the deceived (mobile phone, ID number, personal password, etc.), and then implement transfer, fraud, identity theft, etc. for illegal profit.

Impact on business:

- Loss of customer property
- Being criticized by higher authorities
- Brand reputation destroyed from large-scale phishing attacks

Finance, as the largest attacked industry, can be subdivided into the following attack groups:

4.2.1.1 Against Large-scale Banks

For some large joint-stock banks, attackers usually use real fixed templates (with only logos and pictures changed). Domain names are registered based on certain rules in the early days. But now they gradually tend to be random. Such attacks only target mobile phone users and displaying phishing content only to mobile browsers.

Figure 27: a phishing APP of a large bank

4.2.1.2 Against City Commercial Bank

Active from mid-February 2021 to the present, some groups mainly conduct phishing attacks on city commercial banks, usually using a fixed template (only logos and pictures changed), with certain anti-detection methods. When the page loads, there is only one picture, and the site jumping to the login page. Such operations improve the anti-crawling performance to phishing websites. The attack only targets mobile phone users and displaying phishing content only to mobile browsers. Although the monitoring time is short, the number of monitored risks by Tianji Partners has reached tens of thousands.

Figure 28: a city commercial bank phishing APP

4.2.1.3 Against Securities, Fund and Exchanges

Such groups mainly target phishing attacks on securities, funds, exchanges and other institutions. Compared with the two phishing methods above, these phishing templates used are basically fixed. With little attention paid to anti-detection methods, the lawbreakers initiate attacks in a high frequency. In addition to some well-known stock exchanges attacked, there are also some fictitious organizations that are suspected to be concocted for fraud.

Figure 29: a stock exchange phishing website

4.2.2 Malicious Competitors

Unlike pure "criminal groups", malicious competition is generally generated by competitors whose brands are attacked or counterfeited. This phenomenon is mainly concentrated in industries such as cryptocurrencies, e-commerce and online services. Common use cases include malicious rankings on search engines and counterfeit websites diverting online attention.

Malicious ranking on search engines: Now, search engines have become one of the main ways to obtain information resources online. It is based on this phenomenon that the PPC service in accordance with the level of payment also emerges as the requirements appear. While PPC brings profits to search

engine vendors, it exposes some disadvantages as well. Taking malicious ranking as a example, some companies will use the keywords of competitors to increase the exposure of their own brands, resulting in the phenomenon of "mismatched goods" on search engines.

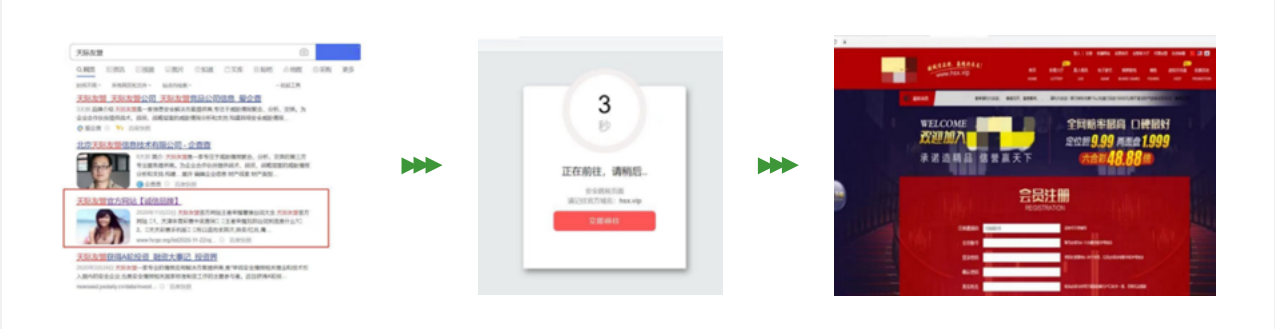


Figure 30: Malicious ranking of a search engine, links to illegal gambling sites

Counterfeit website to divert online attention: It often occurs in the field of cryptocurrency. New things always attract people's attention. It has been noticed that there are some "rising stars" who use the reputation of other brands to create knock-off sites to drive potential customers to their platform.

Figure 31: fake APP of a digital currency trading platform

4.2.3 Illegal Pornography and Gambling Groups

As the name suggests, the main purpose of such groups is to spread pornography and gambling sites which are two types of websites prohibited in China. But for the sake of profit, the groups manage to spread these websites. They have very rich experience in anti-detection, and usually using the codes of official banks websites, governments, and large enterprises as a cover to spread illegal ones. Most of these illegal websites are hosted overseas, most of which do not violate the laws and regulations of the countries where they are hosted, but the "audience" are still netizens in mainland China.

In addition to spreading illegal websites, the groups also make negative impact on the brands of banks, governments, and large enterprises that have been "endorsed". Through technical means, the website source code of the official website is also included in the source code of the illegal website. So that when people searching for the keywords of the official organization, the illegal website has a great possibility to be listed in the search results.

Figure 32: a fake provincial government website spreading football lottery

4.2.4 Malicious Phishing Actors

Malicious intimidation toward Party A is a phenomenon discovered in recent years. In the fight against phishing and counterfeiting, in addition to the continuous confrontation, some special "groups" that are not for mere attacks have also been discovered. According to the current hot phishing attacks, these groups follow the trend to register some similar domain names, and temporarily hosting these phishing websites. Due to the lack of SMS or email phishing transmission, and actual access, the websites do not circulate in the "market" and have a very short life cycle.

However, after Tianji Partners' analysis, these so-called "attacks" generally always occur in the early stage of Party A's bidding or during the bidding period for internet security service. Although with high occurring frequency, there is no actual fraud or attention paid by netizen. Therefore, it is suspected that some security Party B companies have made "self-production and self-selling" behaviors in order to attract Party A's attention to obtain economic benefits.

4.3 By Platform, Service Providers and Demographic

4.3.1 Distribution by Social Media Platforms

The social media detection involves 19 platforms. The listing is arranged in descending order according to the proportion of of each platform in the total number. Among them, Weibo accounts for the largest proportion of 39.85%.

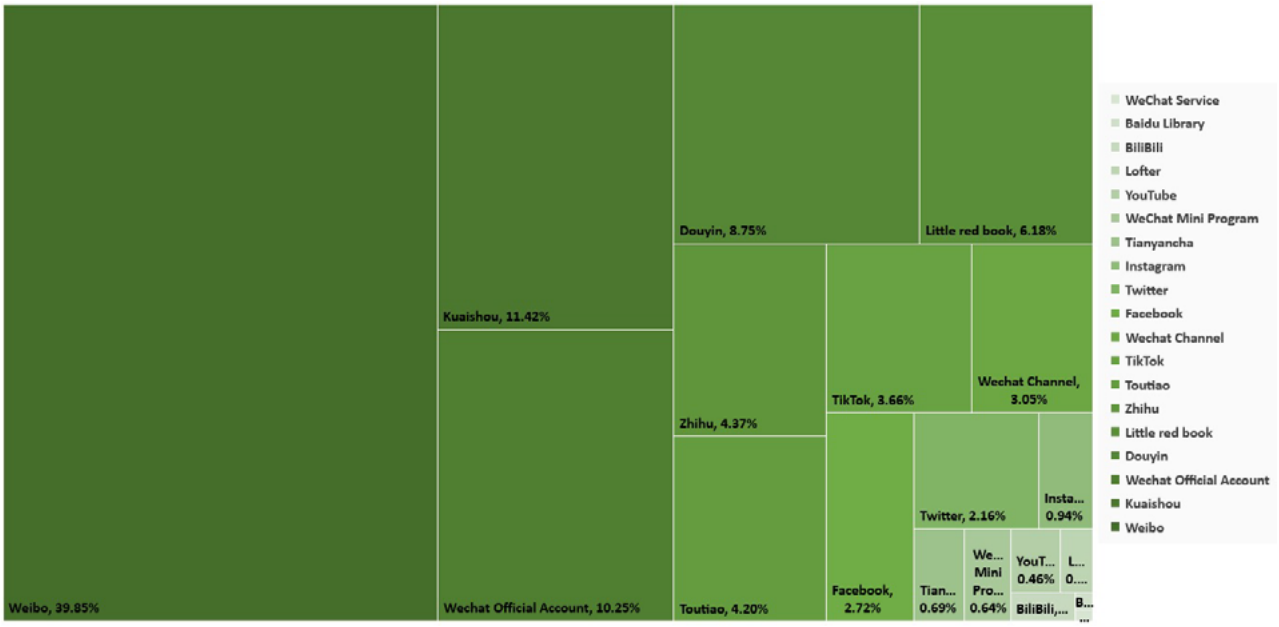


Figure 33: digital risks on social media in 2021

Platform	Quantity	Percentage
Weibo	1,567	39.85%
Kuaishou	449	11.42%
Wechat Official Account	403	10.25%
Douyin	344	8.75%
Little red book	243	6.18%
Zhihu	172	4.37%
Toutiao	165	4.20%
TikTok	144	3.66%
Wechat Channel	120	3.05%
Facebook	107	2.72%
Twitter	85	2.16%
Instagram	37	0.94%
Tianyancha	27	0.69%
WeChat Mini Program	25	0.64%
YouTube	18	0.46%
Lofter	12	0.31%
BiliBili	11	0.28%
Baidu Library	2	0.05%
WeChat Service	1	0.03%
total	3,932	100%

Table 7: digital risks on social media in 2021

4.3.2 Distribution by Mobile APP Stores

The TOP30 mobile APP stores account for 21.25% of all APP risks. The TOP30 is taken as a whole, the listing of which is arranged by percentage. Liqu App Store has the highest proportion, which is 10.4%.

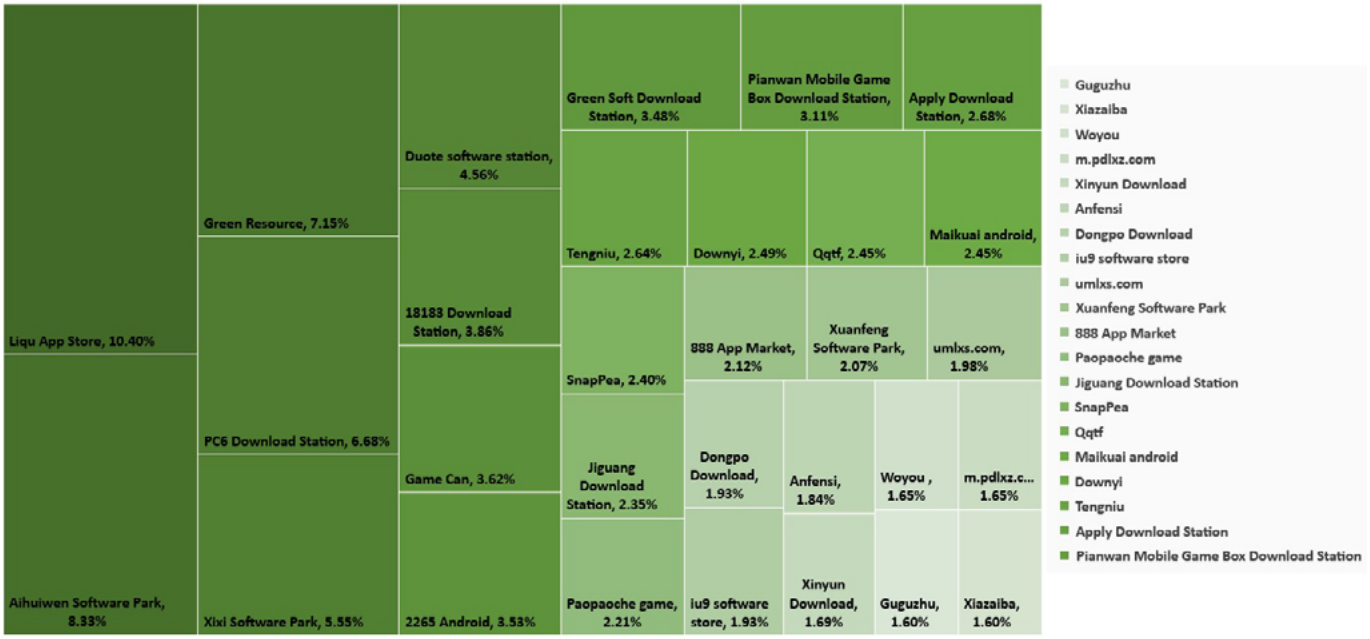


Figure 34: digital Risk in Mobile App Stores in 2021

App Store	Percentage
Liqu App Store	10.4%
Aihuiwen Software Park	8.33%
Green Resource	7.15%
PC6 Download Station	6.68%
Xixi Software Park	5.55%
Duote software station	4.56%
18183 Download Station	3.86%
Game Can	3.62%
2265 Android	3.53%
Green Soft Download Station	3.48%
Pianwan Mobile Game Box Download Station	3.11%
Apply Download Station	2.68%
Tengniu	2.64%
Downyi	2.49%
Qqtf	2.45%
Maikuai android	2.45%

SnapPea	2.4%
Jiguang Download Station	2.35%
Paopaoche game	2.21%
888 App Market	2.12%
Xuanfeng Software Park	2.07%
umlxs.com	1.98%
Dongpo Download	1.93%
iu9 software store	1.93%
Anfensi	1.84%
Xinyun Download	1.69%
Woyou	1.65%
m.pdlxz.com	1.65%
Guguzhu	1.6%
Xiazaiba	1.6%

Table 8: digital Risk in Mobile App Stores in 2021

4.3.3 Distribution by Internet Service Provider

In terms of the Internet service providers that the IPs used by the attacking groups are belonged to, Alibaba Cloud accounts for 21.72% of the total. TOP20 accounts for 68.59 % of the total. TOP20 is listed below:

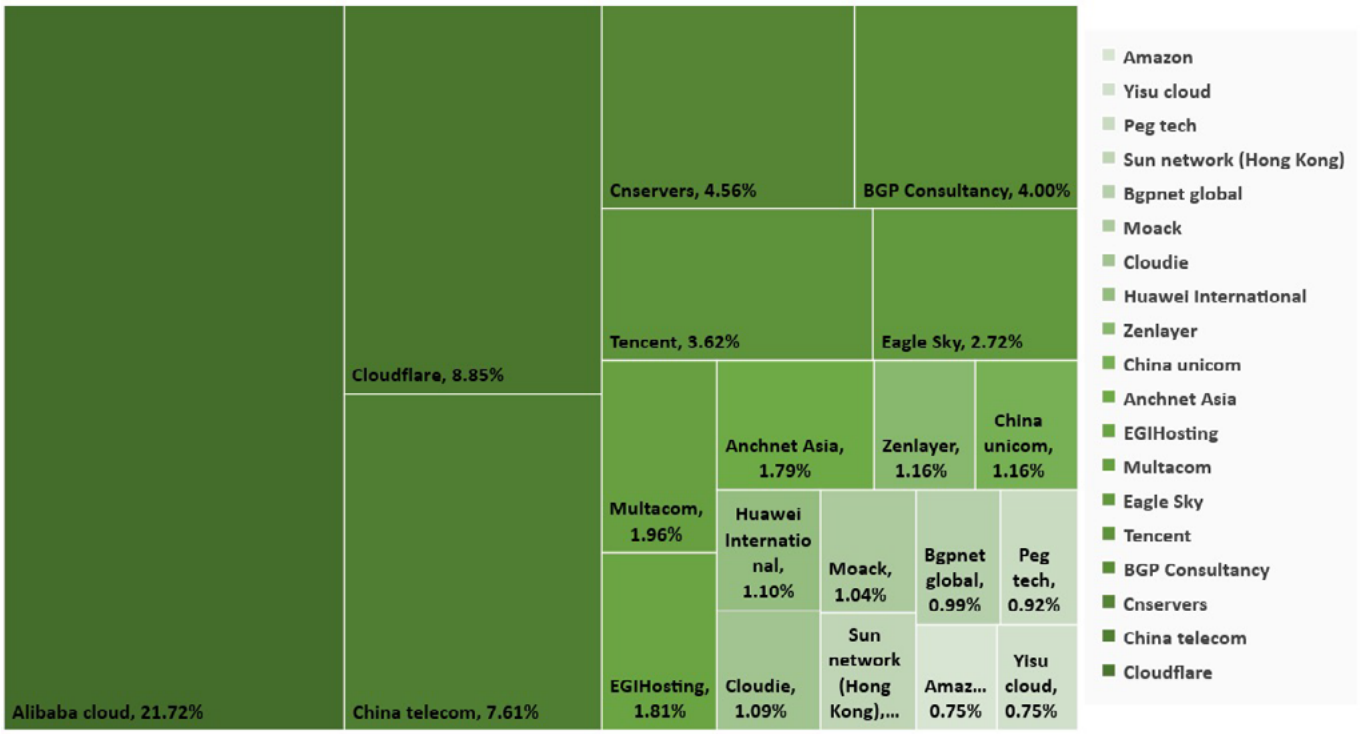


Figure 35: digital risks by ISP in 2021

Internet service provider	Percentage
Alibaba cloud	21.72%

Cloudflare	8.85%
China telecom	7.61%
Cnservers	4.56%
BGP Consultancy	4%
Tencent	3.62%
Eagle Sky	2.72%
Multacom	1.96%
EGIHosting	1.81%
Anchnet Asia	1.79%
Zenlayer	1.16%
China unicom	1.16%
Huawei International	1.1%
Cloudie	1.09%
Moack	1.04%
Sun network (Hong Kong)	0.99%
Bgpnet global	0.99%
Peg tech	0.92%
Amazon	0.75%
Yisu cloud	0.75%

Table 9：digital risks by ISP in 2021

4.3.4 Distribution by Domain Name Registrar

Mainstream domain name registrars TOP20 is presented below. GoDaddy accounts for 16.76%, followed by Alibaba Cloud. TOP20 accounts for 55.49 % of the total.

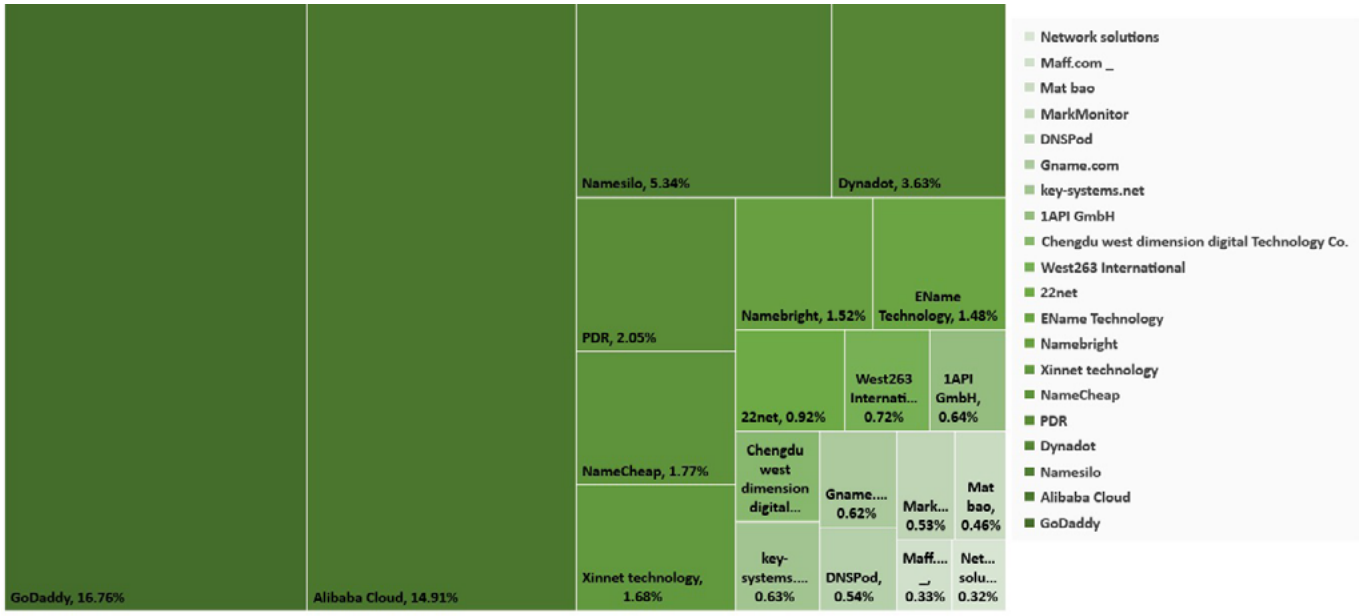


Figure 36：digital risk by major domain name registrars in 2021

Domain Name Service Provider	Percentage
GoDaddy	16.76%
Alibaba Cloud	14.91%
Namesilo	5.34%
Dynadot	3.63%
PDR	2.05%
NameCheap	1.77%
Xinnet technology	1.68%
Namebright	1.52%
EName Technology	1.48%
22net	0.92%
West263 International	0.72%
1API GmbH	0.64%
Chengdu west dimension digital Technology Co.	0.64%
key-systems.net	0.63%
Gname.com	0.62%
DNSPod	0.54%
MarkMonitor	0.53%
Mat bao	0.46%
Maff.com _	0.33%
Network solutions	0.32%

Table 10：digital risk by major domain name registrars in 2021

4.3.5 Distribution by Countries and Regions

According to the geographical distribution of infrastructure IP used by attack groups, total digital risks in various use cases are spread across 97 countries and regions. The following figure shows the TOP20 countries and regions with the highest proportions in descending order.

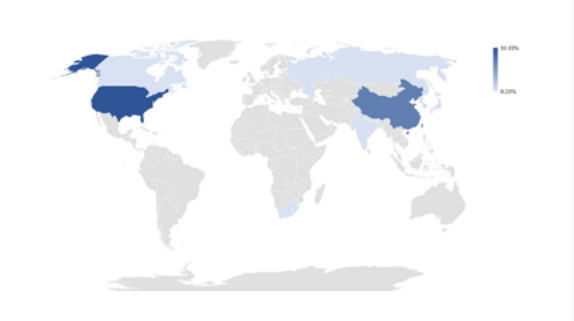


Figure 37: digital risks by countries and regions in 2021

Country and region	Quantity	Percentage
America	25,996	34.65%
Hong Kong China	18,356	24.47%
Chinese Mainland	16,749	22.32%
Singapore	2,465	3.29%
South Korea	1,518	2.02%
Japan	1,337	1.78%
Germany	924	1.23%
Taiwan, China	869	1.16%
India	620	0.83%
Netherlands	585	0.78%
Indonesia	577	0.77%
Russia	574	0.77%
South Africa	452	0.60%
U.K	427	0.57%
France	381	0.51%
Brazil	344	0.46%
Thailand	337	0.45%
Canada	297	0.40%
Malaysia	263	0.35%
Australia	221	0.29%
77 other countries and regions	1,737	2.32%

Table 11: digital risks by country and region in 2021

05 Case Study

5.1 Phishing

5.1.1 Website

5.1.1.1 Common Phishing Website

The criminals pretended to be customer service of a takeaway brand and sent a message to the registered merchants for required authentication, which contained a link to a phishing website, and induced the merchant to enter information such as ID card, bank card, mobile phone number, verification code, etc., so as to steal the their bank cards-. The criminals took advantage of the merchant's concern for handling customer complaints and platform system upgrades, and committed fraud through text messages containing phishing links. Once the victims entered relevant personal information, the bank card would be stolen and swiped, which seriously threatened the property of the deceived.

Figure 38：a reminder for a phishing website issued by The Ministry of Public

Figure 39: phishing website for investment promotion

Figure 40: phishing website for user information

5.1.1.2 New Ransomware URL

Figure 41: Phishing URLs are upgraded to URL ransomware

The malicious website combined domain name spoofing and blackmail into one, not only highly

imitating an investment company's official website domain name to confuse users, but also forcibly locking all accessed PCs with security vulnerabilities, so as to offer paid unlocking assistance. After the user who installed the protection software agreed to install the malicious plug-in, the files on the PC would also be forcibly locked. After Tianji Partners' effort, the current visit to the target website jumped to other websites, but malicious programs failed to be downloaded.

5.1.2 Mobile APP

5.1.2.1 APP Advertisement

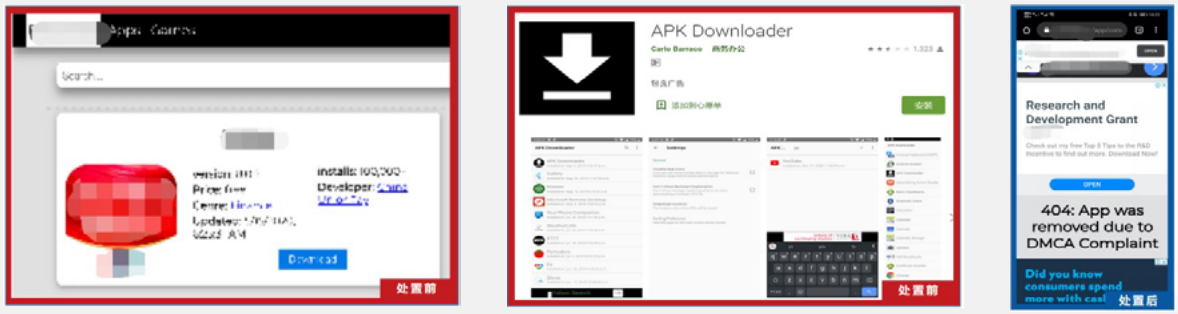


Figure 42: unauthorized payment APP

An app store launched a well-known payment app without authorization. After downloading and installing the app, it was found that the actual app was APK Downloader (a fake app store, which tricked users to click on ads to attract traffic and get advertising fees, but did not actually generate any download behavior), and no other malicious behaviors found. In addition, after in-depth investigation, all APPs in the download site were the same Adware APP (APK Downloader), and the download function of this APP actually existed for google ads. The platform was suspected of counterfeiting the official APP, which was a trademark infringement. Moreover, without any money fraud reported to the brand service, it was suspected of no fraud involved. After Tianji Partners' takedown, the infringing APP was taken off the market and could not be searched.

5.1.2.2 Unauthorized APP

Attackers develop counterfeit apps, abusing brand logos and trademarks, and distributing through unauthorized channels to steal various victim users' bank card, identity, passwords and other private information.

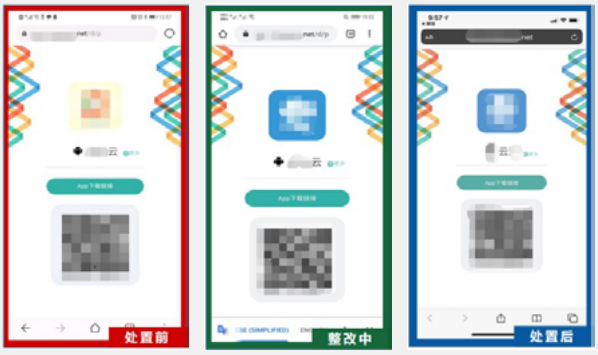


Figure 43: unauthorized APP of a cloud service company

5.1.3 Social Media

5.1.3.1 Phishing on WeChat

According to WeChat rules, a fake public account, although through verification, can be taken offline after the evidence of infringement submitted to the platform.

Figure 44: a fake public account on Wec

According to WeChat rules, a fake public account, although through verification, can be taken offline after the evidence of infringement submitted to the platform.

Figure 45 shows a WeChat personal account without verification, rather than a public account. According to the platform rules, if sufficient evidence of fraud cannot be provided, only a warning can be issued to require the removal of the infringing content. After the warning, the target account stopped the usage of the involved brand logo and content.

Figure 45: a fake customer service account on Wechat

5.1.3.2 Phishing on Xiaohongshu

An account on Xiaohongshu exploited the name of a well-known bank, which is considered as brand infringement. After takedown, the account deleted infringing content.

Figure 46：a phishing bank account on Xiaohongshu

5.1.4 Email

5.1.4.1 Official Email address

The official service email address of a well-known logistics company was hacked and used to participate in phishing. The takedown means was to stop domain name system or stop mail

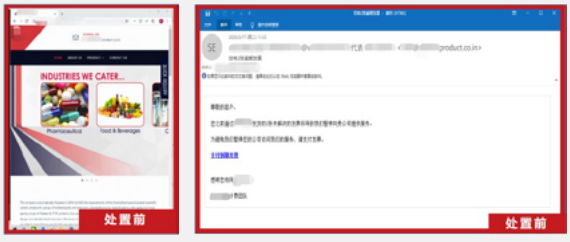


Figure 47: An official customer service email address forcibly“participated in” phishing

function. Due to the concern that an abrupt termination of email service might influence a large number of customers, the company needed to go through an internal evaluation and procedure, and did not yet handled it.

5.1.4.2 Phishing Emails

In this case, the phishing email used by the criminals was highly similar to the official service email of a well-known short video platform. The phishing email sent paid promotional information to trick users into clicking on the phishing website embedded in the email to steal users' private information, bank card, etc. data. After takedown, the domain name of the email address was stopped operating, and the embedded phishing website in the fraud email could not be accessed. At the same time, the email service was suspended.

Figure 48: phishing email address similar to the official address

5.2 Brand Abuse

5.2.1 Website

5.2.1.1 False Advertising

The infringing website falsely advertised its partnership with a famous trading platform and used the platform's registered trademark without authorization. The purpose was to use the infringed website reputation to promote itself for profit.

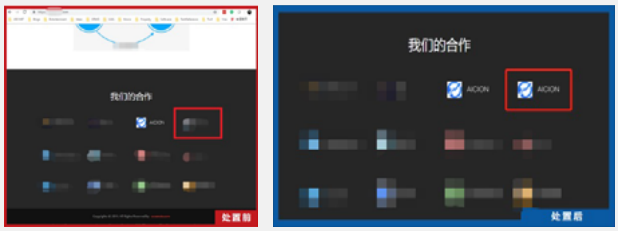


Figure 49: a website suspected of false propaganda

5.2.1.2 For Pornography, Gambling and Drugs

The brand name of a short video website was abused by a infringing website to divert online traffic to the pornographic resources of its own website, which had a negative impact on the brand company and damaged the brand image. After takedown, the infringing content was completely deleted.

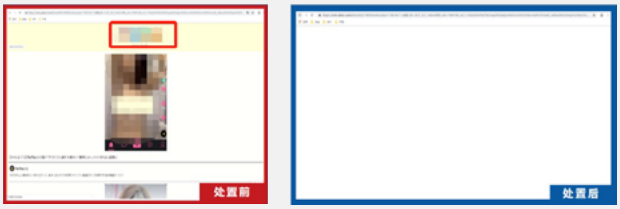


Figure 50: brand abuse for pornographic websites

5.2.2 Mobile APP

5.2.2.1 Falsely Advertising

In addition to website, APPs may also be detected for falsely promoting partnerships. Usually, brand infringement is displayed at the end of the APP homepage.

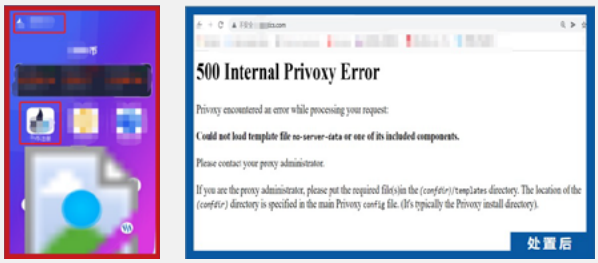


Figure 51: APP trademark abuse

5.2.2.2 Non Existing Fake APP

A company in Hangzhou received reports that criminals had exploited its corporate name to create and publish financial investment and wealth management apps, resulting in many users' losses. The company issued a statement to clarify that it had never developed and launched any financial management app, and the app in question committed a trademark infringement. In order to maintain the brand image and prevent more victims from economic losses, the brand party involved reported it to the police department.

Figure 52: fake APP of a technology company

5.3 Copyright Piracy

The evolution of piracy is staggering. With the advent of the Internet age, traditional pirated books, magazines, video discs, software installation disks and other entities have gradually withdrawn from people's attention, and slowly transformed into digital forms and re-entered the lives of the public. Although this digital transformation has provided convenience for companies and audience to a large extent, the problem of piracy has also grown and intensified with the development of the Internet. Film and television, variety shows, competitions, music, office software, games, photography, etc. have not been spared. Taking the hardest-hit film and television as an example, from pirated video discs from many years ago to resource links offered by social media nowadays, the problem of piracy has been plaguing the entity and digital fields all along.

5.3.1 On Live Streaming

Since the day the Internet entered the public eye, various online theaters have always been one of the main ways to obtain pirated resources. The creation and maintenance of such websites do not require advanced technical capabilities, however with low cost and high advertising revenue. Normally, there are online templates for website establishment.

Figure 53: pirated resources on websites

5.3.2 Resources on Cloud Storage

The rise of netdisk has brought great convenience to resources sharing among netizens, but also provided a channel for the dissemination of pirated resources. Audience can download large-capacity high-definition film sources via netdisk to improve viewing experience. If these film sources are watched online, the loading progress may be hindered by internet speed, and the viewing experience will not be satisfying.

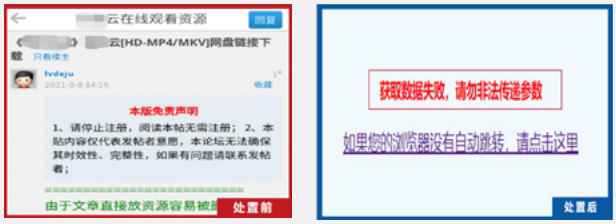


Figure 54: pirated resources of an international movie on Cloud Storage

5.3.3 BT Download

BT torrent downloads were all the rage many years ago, but now with the development of the Internet and the emergence of various new platforms, although BT torrents are commonly found in forums, their status has already plummeted. There are many reasons for this, one of which is limited download speed. The download software offers high-speed downloads for paid members, but membership fees are expensive. Audience with insufficient funds may take a day or more to see their favorite movies, but the mood of entertainment at that time has been seriously frustrated.

Figure 55: BT pirated resources of an international movie

5.3.4 Social Media

The pirated resources on social media are not only easy to obtain, but also take advantage of the characteristics of their platforms, combined with the fragmented time of users, attracting the attention of audience. Social media breaks the time and geographical restrictions, and provides netizens with maximum freedom to watch movies.

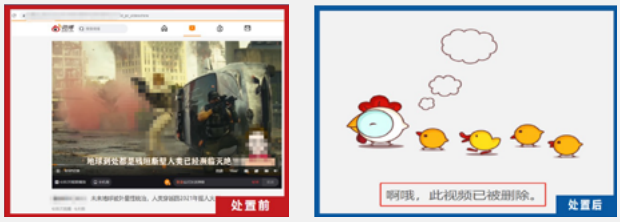


Figure 56: pirated resources of an international film on social media

5.4 Data Leakage

5.4.1 Document Sharing Platforms

The library platform is the hardest hit area where leaked data spreads. A large number of uploaders improperly profit from publishing corporate confidential documents, which not only damages the reputation of the company, but also causes a serious threat to technological achievements and program performance.

Figure 57: a program report leaked on a online library

5.4.2 Websites

Some data breaches that occur on websites are not spread in the form of publicly downloaded documents, but are directly published on the website for free viewing to attract attention.

Figure 58: paid knowledge published free of charge on a website

5.4.3 Cloud Storage

Customer information, market strategies, technological inventions and other core internal materials have been illegally stolen and publicly disseminated on platforms such as cloud storage, which not only directly damaged the enterprise interests , but also affected the security and brand reputation.

Figure 59: implementation plan on Cloud Storage

5.4.4 Copyright Infringement

During the coronavirus epidemic, the demand for online education has explosively surged. Some leading brands took the opportunity to create a reputation. However, the low-priced documents are also rampant. Online courses worth of thousands CNY are put on knowledge sharing websites and forums, or then sold through platforms such as Xianyu and Baidu Tieba with only a few cost. This phenomenon has seriously affected the platform's membership plan and business profit, and also destruct the creative enthusiasm of producers.

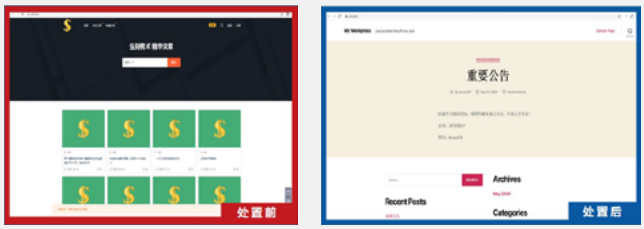


Figure 60: paid article stolen by another knowledge platform

5.4.5 Social Media

Many criminals use social media to spread paid content in an attempt to expand their contacts with netizens. This kind of behavior not only causes business losses to the copyright owners, but also damages their brand image.

Figure 61: Paid lessons sold without authorization on WeChat

5.5 Code Leakage

5.5.1 Code Leakage on Github

The code data of a bank concerning good return service was publicly shared on Github. The disclosed code might not only be used by malicious personnel to attack and extort the brand's service system, but also cause economic fraud to consumers and seriously affect the brand image. After takedown, the leaked code was removed from the Github.

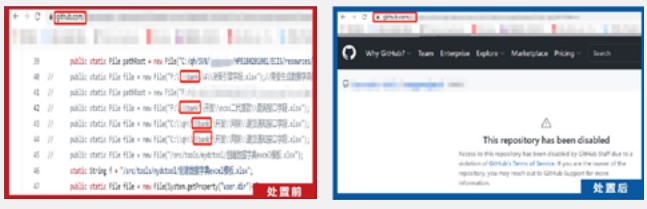


Figure 62: internal system code of a bank shared on Github

5.5.2 Code Leakage on Gitee

Gitee is another hot spot for code leaks. A bank's video conference software solution interface code was posted on Gitee for viewing free of charge. External threats could easily use code loopholes to monitor important meetings, and obtain network data of participants, resulting in a serious network security crisis. After takedown, the code involved was removed.

Figure 63: a bank's meeting software code shared on Gitee

5.6 False Positives Rectification

5.6.1 False Positives of Website

5.6.1.1 On PC

Tencent Security monitored an official website and marked it as dangerous. After negotiating with the Tencent Security Center, it was suspected that the website had been maliciously reported, and it would restore after Tencent's approval progress. The progress would take 30 working days after application document submission.

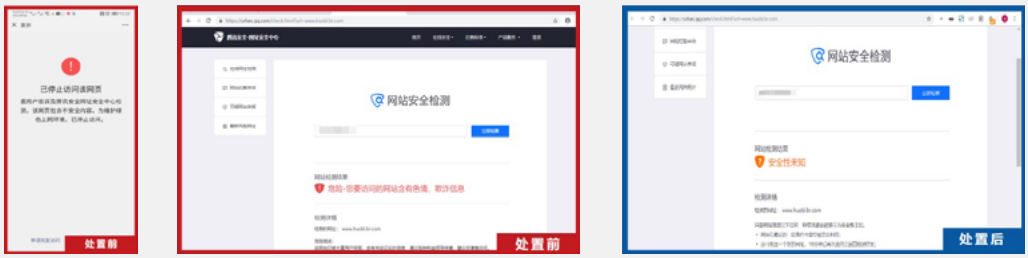


Figure 64: Tencent Security Center misjudged an official website

5.6.1.2 On Mobile Safari

An APP of a trading platform downloaded on browser on Huawei mobile phones was falsely reported as a threat subject. The false positive was removed after 15 working days since restoration application.

Figure 65: Huawei mobile browser misjudged an official website

5.6.2 Mobile APPs

When an APP provided by official mobile phone web page is installed on an Android phone, it is reminded to be risky software. This warning will mislead users to stop using the APP, and will seriously question the brand's reputation, causing a certain loss of customers and damaging the brand image. After restoration application, normal download resumed after 3 natural days, with no risk warning.

Figure 66: the Android mobile system misjudged an official website

06 Comparing Digital Risks in and outside China

Digital risk is a global problem

From an enterprise's point of view, if a company's business is to serve global users, the assets will inevitably be exposed on the entire Internet. From the perspective of attackers, they often hide in countries where the law-breaking activities do not occur to evade regulatory sanctions. For example, organizations or groups that target Chinese companies for fraud usually register phishing websites outside China. In this way, even if the target company finds out that the website has been phished, in most cases it is powerless to shut down timely and effectively.

Tianji Parners has been engaged in international digital risk protection practice for many years with rich experience. Based on the practice in the past few years, we summarize some differences in digital risk protection between China and oversea countries from the following dimensions.

Perspectives	Difference	Description
Attack target	Financial sector	"Overseas: Most of the phishing attacks in the financial sector target large-scale commercial banks. Foreign advanced attack groups prefer online banking Trojans. Those who only focus on phishing attacks are fraud groups with merely basic techniques. Domestic: The financial sector is still the main target of phishing groups. The Internet environment, the mobile banking popularity, and language barriers have made it impossible for online banking Trojans to be widely applied by attackers. Therefore, as for the financial sector, especially banks and securities enterprises, attackers will still rely on various phishing methods to steal identities and sensitive information. At the same time, for domestic netizens' lack of security awareness, simple phishing attacks succeed easily."
	Internet online service	"Overseas: Large-scale online service platforms are only a few, while others are basically small and unfamous. So the attacks are mainly concentrated on several large e-commerce websites (such as ebay, amazon, etc.). Domestic: For the rapid development of the Internet, except for a few large e-commerce platforms, online food ordering and express delivery are widely spread. Because of the full life aspect coverage of online servicez, the attacks scope is relatively wide as well."

Propagation mode	E-mail	"Overseas: Since business communication via email is popular, the phishing email still remains a mainstream attack method. Domestic: With the rapid development of mobile office tools, email is no longer the mainstream communication way. Instant messaging apps and cooperative office platforms (such as DingTalk and Wecom) are more popular emails for better efficiency. However, email is still relatively common in foreign trade and multinational businesses, and it will still remain a attack target."
	Short message	"Overseas: The main way of spreading phishing attacks is through emails, and some of them are through social media. But, short messages is not widely used. Domestic: Compared to emails with less popularity, phishing attacks through short messages are nationally applied for massive audience and wide uasge of mobile phones."
	Social media	"The differences mainly rely on distinct social media platforms. Overseas social media platforms with high digital risks: Facebook, Twitter, Instagram, Linkedin, etc. Domestic social media platforms with high digital risks: Weibo , WeChat public account, Toutiao, Douyin, Xiaohongshu, Kuaishou, etc."
	Mobile APP	"As for the iOS system, due to the unified management, there are basically only official APP stores across the world. For the Android system: Overseas: the general understanding of the official APP download channel is google play, and other stores are regarded as third party stores. In China, the Android system does not have a designated official APP store. Almost every major Android mobile phone manufacturer in China has its own APP store, and many famous Internet enterprise have launched APP stores. However, due to the different security standards in each store, the developer identity verification and the software security regulations are different. Therefore, many apps with mallicious malware can be obtained from some third-party APP stores."
Attack features	Infrastructure	"Overseas: The infrastructure of phishing attacks mainly include zombie computers and free hosts. These two types accounted for almost 90% of overseas phishing attacks 10 years ago. In recent years, maliciously similar domain name have gradually emerged. Although the proportion is on the rise, it is not a mainstream attack method. Domestic: Most phishing attacks use similar malicious domain names, the cost of which is much higher than that of zombie computers and free hosts. And the attack is more difficult to deal with. This can ensure the persistence of the phishing attack process and strive for more opportunities and time for attackers."
	Template design	"Overseas: usually different website templates for different targets. Domestic: Domestic groups often use the same template to carry out attacks of several brands. Although with highly repeated appearences, attacks are more efficient and the probability of being blocked or complained is not as high as immagined."

Development status	Party A's attitude	"Overseas: Foreign companies have a relatively strong awareness of brand protection and will take the initiative to build a safe brand image. The demand for digital risk protection generally comes from their own pressure from external threats and security protection. And relevant legal system and support is mature. Domestic: The demand for digital risk protection by domestic privated companies and government-sponsored institutions originates from external pressures such as compliance. Usually, actions are taken only when policies require, and only when the companies and institutions are notified by inspection departments."
	Intelligence Sharing Mechanism	Overseas: Overseas service providers share a lot of intelligence in English, and detection mainly focuses on data analysis and optimization. However, due to lack of language ability and different customer groups, it is rare to find risk data for Chinese brands. Domestic: Intelligence is in the hands of a few service providers, and there is no mature intelligence sharing mechanism. Detection mainly relies on the detection mechanism independently developed by service providers. And only a few manufacturers provide detection and take down service for digital risk protection.

07 Guide to Digital Risk Protection

With the rapid development of the Internet, digital transformation has become an unavoidable challenge for the whole society. The COVID-19 pandemic that swept the world in 2020 has accelerated this process. However, digital transformation also brings a variety of digital risks, and the digital assets of enterprises and institutions are also facing more external threats.

In the era of digital economy, the demands of various entities for digital risk protection are increasing day by day. Organizations need a standard, disciplined approach to newborn digital risks in order to satisfy the maturity requirements for risk management. The IDRR framework is a life cycle-based digital risk protection methodology that combines with the information security framework to effectively solve problems and challenges mentioned above.

7.1 Digital Risk Protection Framework (IDRR Framework)

The IDRR framework, based on the digital risk protection life cycle, is divided into four stages: Identify, Detect, Response, and Recovery. This model integrates continuous improvement into the digital risk protection model, which provides enterprises with full life cycle management of digital risks.

Identify(I): "Identify" means understanding the cybersecurity risks of organizational operations (including mission, function, image or reputation), organizational assets and individuals, identifying and managing of enterprise assets elements and their importance to business objectives to supports operational risk decisions. Specifically, "Identification" can be divided into four steps:

Firstly, identify valuable digital assets. It is crucial to establish a management team to sort out the valuable digital assets of the enterprise. Enterprise assets include but are not limited to websites, domain names, official APPs, social media accounts or executives' personal social media accounts, as well as corporate internal data, files, codes, etc.

Secondly, evaluate the footprint and exposure of digital assets. After the asset sorting, professionals will evaluate the dissemination and exposed surfaces of the digital assets on the Internet according to the website domain name whitelist, official APP domain name whitelist or authorized download channel whitelist, keywords, digital watermarks, HASH, specific strings, etc.

Thirdly, digital risk and loss analysis. It is suggested to analyze the risks that enterprise digital assets may or have faced, and to calculate in advanced the losses that may or have been caused to the enterprise.

Fourthly, develop a digital risk protection strategy. According to the digital assets that enterprises are

concerned about, corresponding protection strategies are necessary.

Detect(D): "Detect" indicates the comprehensive monitoring of an enterprise's information, assets, and digital footprints to identify cybersecurity incidents and abnormal activities, understanding the potential impact of incidents, and evaluating incident risk levels.

The monitoring capability depends on two systems. One is intelligence system, including NOD (newly observed domain names), threat intelligence, third-party intelligence, dark web intelligence, etc. The other is the technical system, including crawler confrontation, NLP (natural language processing) , image recognition, audio recognition, video recognition and other technologies.

The monitoring objects target two types of assets. One is hidden assets, including detection scanning, remote control, malicious emails, IDS, SIEM/SOC, situational awareness, etc. The other is exposed assets, including domain name security, mobile apps, corporate social media accounts, executives' social media accounts, data, code credentials, search engines, etc.

Response (R): "Response" refers to implementing response procedures to prevent incident spread, to mitigate impact , to communicate and coordinate with internal and external departments, including seeking external support from law enforcement agencies.

The specific process of response is to deal with threats such as phishing and counterfeiting, brand infringement, data leakage, and threat false positives that digital assets may face. It is necessary to communicate and cooperate with application store managers, and social media platform managers to quickly shut down the above digital risks, and continuously track the take results to ensure the complete eradication of digital risks.

Recovery (R): "Recovery" means coordinating recovery activities with internal and external parties, and implementing recovery processes and procedures to ensure timely recovery of systems or assets affected by a cybersecurity incident. Occurred risks are recorded to improve recovery plans. On the other hand, it is essential to be capable of early warning and second takedown when continuous monitoring of target brands or assets on the Internet discovers a risk of "resurrection". Therefore, the risk of exposed assets can be controlled, stable and safe.

Full Life Cycle Management of Digital Risk

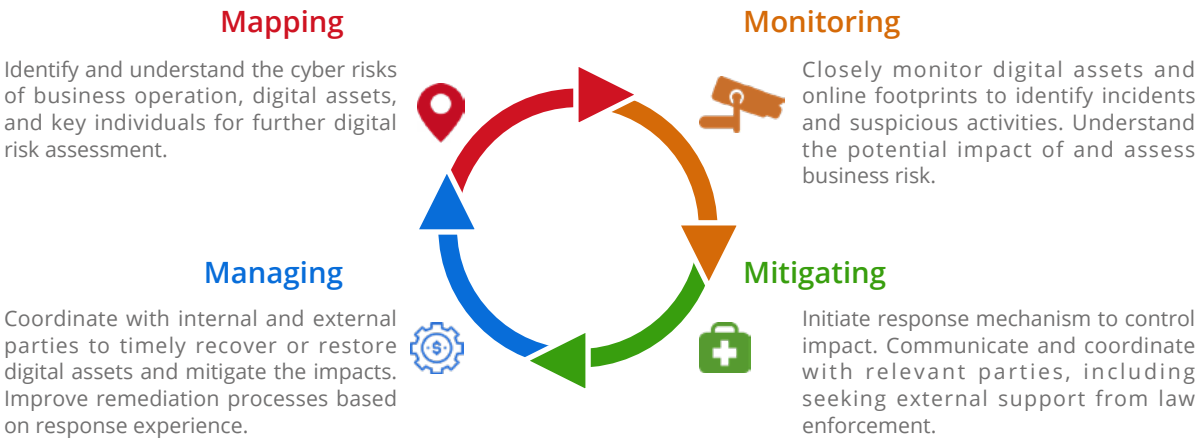


Figure 67: the full life cycle of digital risk management

7.2 Industry Needs for Digital Risk Protection

With the development of the digital economy, any industry, any enterprise, and any institution may encounter numerous external threats and digital risks. Enterprises, institutions and other entities have an increasing demand for digital risk management. According to Tianji Partners' observation and research, the industry of finance, film and television entertainment, digital asset, paid digital content, large state-owned enterprises and governmental institutions are more vulnerable to different types of digital risks due to the particularity of each industry. The requirements are manifested in business operation and regulation.

7.2.1Banking and Finance

The financial industry, because of its particular business attributes, has always been a key target of various counterfeiting and fraud. Digital financial fraud methods show new characteristics such as specialization, industrialization, concealment, and scene-based. According to the APWG report in the fourth quarter of 2020, phishing against financial institutions are still the most common attacks. Attackers use URL similar to authentic website of enterprise, dedicated to steal bank card, identity, passwords and other private information.

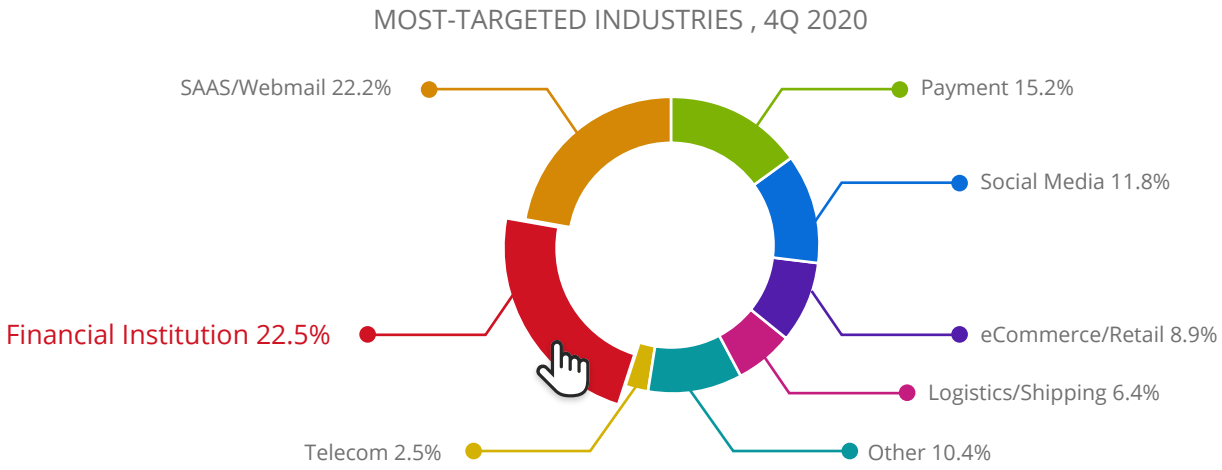


Figure 68: Phishing attacks targeting financial institutions are the most prevalent

Digital financial fraud is a problem that an industry and the entire society need to face. Financial regulators have clearly stipulated that financial institutions must strengthen security technical precautions, strengthening the construction of active detection of phishing websites, actively searching for phishing websites, and taking multiple measures to shut down phishing websites in a timely manner, otherwise they will be publicly criticized by regulatory departments. As early as 2011, the China Banking Regulatory Commission issued the "Notice of the General Office of the China Banking Regulatory Commission on Further Strengthening the Risk Prevention and Control of Online Banking". All banking financial institutions should attach great importance to the risk and online banking management, and strengthening the prevention of "phishing" frauds such as counterfeit websites. At the same time, to prevent incidents, it is important to strengthen the construction of an anti-phishing emergency response mechanism to effectively cut off the phishing fraud channels. In 2020, People's Bank of China issued "General Specification for Information Security for Internet Banking System".

The specification specifically emphasized the requirements for "anti-phishing":

- Financial institutions should be anti-phishing
- Technical measures such as anti-phishing website controls, phishing website monitoring tools, and phishing website discovery services should be taken to monitor and discover risks in a timely manner, and establish a mechanism for reporting phishing website cases and quickly taking down phishing websites
- Anti-phishing application control and risk monitoring measures should be strengthened

Figure 69: "General Specification for Information Security for Internet Banking System"

During the pandemic, in order to comply with the requirements of pandemic prevention, people tried their best to use the Internet to complete daily activities such as shopping and working to go out less. Compared with “the past”, the scope of use and transaction amount of digital CYN are also increasing. On the other hand, people's living standards have skyrocketed with savings gradually accumulated, and their awareness of financial management has also become stronger. The love for investment products also tends to be evident in both the elderly and the young. Online banking not only helps people complete transactions, but also provides a platform for wealth management. Therefore the usage in people's lives is gradually increasing. Many criminals grab this opportunity, creating a large number of phishing websites and phishing APPs that imitate real banks websites, and deceiveing users' trust, so that users log on to the fake platform with bank card or sensitive information stolen, which leads to financial loss.

Figure 70: phishing website imitating a well-known bank

Figure 71: Counterfeit APP of a local bank

Common digital risk use cases in the financial industry include:

Phishing Fraud

Brand infringement

Data breach

7.2.2 Film and Television Entertainment

In recent years, digital works (including movies, novels, sports, animation, pictures, music, games, etc.) have been pirated one after another, and the phenomenon has become more and more intense. After the digital works of enterprises are illegally stolen, they are publicly spread on websites, netdisk, social media and other

platforms, which causes heavy losses to the copyright owners and publishers.

Figure 72: the movie "The Wandering Earth"

Taking film and television piracy as an example, it may occur at different stages such as production, distribution, and release, with huge losses to producers, distributors, theater chains or authorized broadcasting platforms, and seriously affecting the film and television industry. Guo Fan, the director of "The Wandering Earth", once told the media that in order to prevent piracy, three anti-piracy teams adopted an extreme encryption at every production stage and kept continuous piracy monitoring after film launch. However, the reality showed that piracy was still hard to prevent. Gong Gem, the film's producer, said in an interview with the media, "We estimate that all the Spring Festival films have been viewed more than 20 million times online. This is very conservative, because peer-to-peer downloads cannot be counted." With a ticket worth of 46 CYN(average price provided by Maoyan), the pirated resources of "The Wandering Earth" causes a loss of more than 900 million CYN. It is estimated that the total box office loss caused by piracy in the 2019 Spring Festival is as high as 1.52 billion.

Film and television piracy can occur at any stage of film production, distribution and broadcast. Most of the pirate teams will cross-disseminate through various platforms such as overseas websites, Weibo, official accounts, and netdisks. This combination of upstream and downstream technology and distribution enables pirate organizations to operate efficiently, and at the same time brings significant economic profit.

Piracy groups are technologically advanced, highly concealed, and pirated resources are spread around the world in various forms and complicated to be shut down. The traditional filtering technology may not be useful with problems suspended. Traditional legal means are effective for large piracy websites , but helpless for small overseas ones. No matter how hard the piracy groups crack the encryption, extracting the code stream or copying illegally in the early stage, and how far to spread it through social media, second-hand trading platforms and other platforms in the mid-term, the ultimate goal is to obtain commercial benefits.

Common digital risk use cases in the copyright industry include:

Copyright Piracy

Brand infringement

Celebrity counterfeit

7.2.3 Digital Asset

At present, the development of the global digital economy is in a stage of rapid advancement. According to "Analysis Report on Market Prospects and Investment Planning of China's Digital Economy Industry" released by Forward Business and Intelligence Research Institute in 2021, the proportion of the digital economy in global GDP is expected to exceed 60%. According to IDC's forecast, by 2023, the output value of the digital economy will account for 62% of the global GDP, and the world will enter the era of the digital economy.

With the development of the digital economy, digital assets are gradually showing their vitality, becoming one

of the most active asset forms in the economic and financial field, highly valued by many parties including the government and market institutions. The value of digital assets in the economic and financial market is also increasingly prominent.

2021 is a critical year for the development of the digital asset. On the one hand, encrypted digital assets have ushered in explosive growth. The research and development process of legal digital currency in many countries and regions has accelerated. Among them, E-CNY has an outstanding performance and is currently in a leading position in the world. By March 18, 2021, E-CNY has carried out seven rounds of pilots in Shenzhen, Suzhou, Beijing, Chengdu and other places, with a total of 150 million digital currency issued.

Because of the particularity of the digital asset industry, relevant entities are vulnerable to various types of targeted attacks and frauds, and well-built brands may be destroyed in an instant. Therefore, the industry's need for digital risk protection is becoming more and more urgent. According to Tianji Partners' observation, there has never been an industry that has suffered so many types of attacks. It is rare to witness attackers skillful at such complex and concealed techniques, and the risks with the features of time sensitivity, technical confrontation, repeated "resurrection" and target switching in same industries. For example, criminals will pretend to be the company's customer service or use a fake official account on WeChat to carry out phishing and fraudulent activities and ultimately cause economic losses.

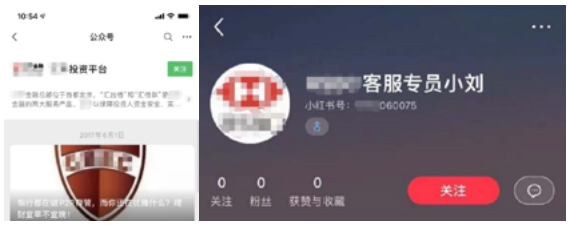


Figure 73: social media phishing fraud risk for a bank

Common digital risk use cases in the digital asset industry include:

Phishing Fraud

Brand infringement

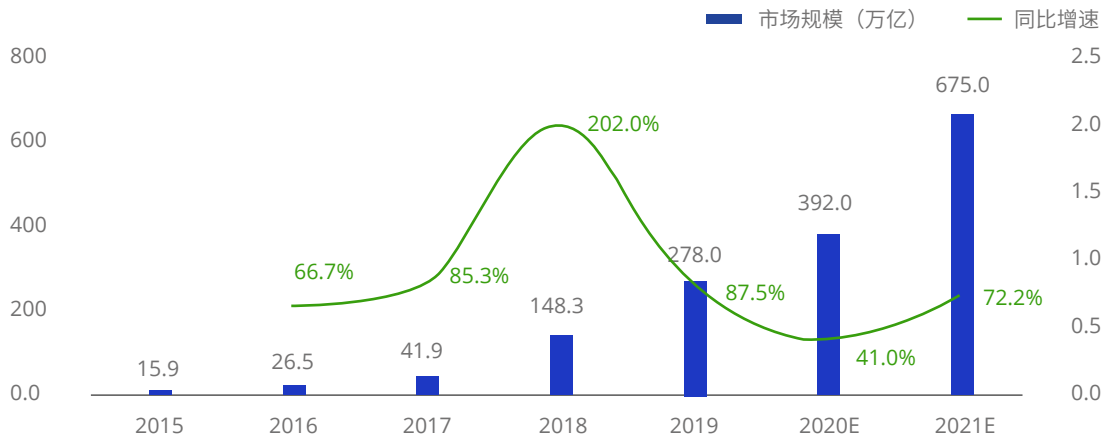
Data breach

Search engine malicious ranking

False positive

7.2.4 Paid Digital Content

With the development of the Internet, paid digital content in China has risen and developed in various operating forms. For example, Zhihu in the expert model, Douban with the form of opinion leaders, as well as open classes, communication communities, and professional classes on apps in various fields such as fitness, painting, and art, etc. Affected by the pandemic, 2020 has witnessed the explosive growth of the knowledge payment industry. According to the "Report for 2020-2024 Chinese digital content payment Industry Research and Investment Forecast" released by the China Investment Industry Research Institute, the scale of Chinese digital content payment market will reach 39.2 billion CYN in 2020, and it is expected to exceed 67.5 billion CYN in 2021.



Data source: iiMedia Research Consulting

Figure 74: 2015-2021 China's digital content payment market forecast

At the same time, digital content payment has also become the hardest hit area of online copyright infringement. Taking online courses as an example, criminals use screen recording, technical cracking, etc. to transfer the online course resources to e-commerce, second-hand trading platforms, and social groups for selling, causing enormous losses to copyright owners.

In the network environment, the complexity and particularity of intellectual property make the protection work come across new challenges. Although the "Copyright Law", " Regulation on the Protection of the Right to Communicate Works to the Public over Information Networks" and other intellectual property laws and regulations, as well as criminal Law and civil procedural Law have been revised and improved, the means of copyright infringement often have a high technical threshold. There are many multi-national and cross-regional crimes, with concealed profit method, and the target is also market-selective. This objectively results in scattered evidence, making it difficult for rights holders or public security departments to find necessary and critical first-handed evidence in the case proceeding.

Common risks in the paid digital content include:

Brand infringement

Data breach

Search engine malicious ranking

7.2.5 Large State-owned Enterprises

In the past few years, large-scale data leakage incidents have emerged one after another. The whole society have paid increasing attention to the security of data assets. The worldly pandemic has brought the cyber threat situation increasingly severe.

As the developing informatization of large state-owned enterprises, data has become the core asset of the organization. While fully enjoying the dividends brought by the "Sword of Damocles" of information technology, state-owned enterprises that master the lifeline of the country's economy also encounter the risk of data leakage, especially the highly concentrated information infrastructure constructed by cloud computing and big data. The risks posed by system fragility cannot be ignored. Once the core classified information such as enterprise product technological development, market strategy, etc. is leaked, it will not only directly

lead to damage to the interests of the enterprise, but also may cause major security problems and serious negative impact on the brand. At the same time, personal data is also one of the core assets of enterprises. While emphasizing rights, enterprises also have responsibilities and obligations to protect users' private data.

Figure 75: a fake website of a large national energy company promoting illegal gambling

In 2014, General Secretary Xi put forward the guiding ideology that "without cybersecurity, there will be no national security". In order to adapt to the increasingly severe network security situation, various countries continue to strengthen their efforts to protect data. China has successively issued policies and regulations such as “cyberspace security strategy”, “Cybersecurity Law”, and others such as the “Data Security Law” and “the Personal Information Protection Law” are also being formulated. These laws and regulations urge the whole society, especially state-owned and central enterprises, to strengthen the construction of network security, protect the core data assets of enterprises, improve the management mechanism, raise security awareness, take effective measures to reduce the probability of leakage of sensitive information, and improve the core competitiveness of enterprises.

Common digital risks for large state-owned enterprises include:

Brand infringement

Data breach

7.2.6 Government

Government departments and agencies include public security, taxation, education, and medical care, etc. These agencies and educational institutions, such as universities and colleges, have certain authority and are easy to gain the trust of the general public. Therefore, web page tampering and infringement incidents against such subjects occur frequently. For example, a website pretended to be a government website, publishing a large amount of false information in violation of regulations, misleading netizens, and causing negative social impact. Another website imitated a law enforcement website for certificate inquiry and personal information collection, which severely violated the legitimate rights and interests of citizens. Furthermore, there were also some counterfeit websites that contained pornographic, gambling information in the name of governmental departments. The above subjects violated the "The Cybersecurity Law of the People's Republic of China", "Regulation on Internet Information Service of the People's Republic of China" and other regulations, and seriously interfering with the order of online information dissemination, damaging the image and credibility

of government departments, universities and other institutions, and endangering the interests of the masses.

Figure 76: a fake website of a provincial tax bureau

In 2018, the Ministry of Industry and Information Technology issued the "Notice on the Further Work on the Prevention Communication and Information Fraud". One of the important tasks is to strengthen the rectification of phishing websites and malicious programs, effectively reduce the risk of online fraud, strengthen the monitoring, analysis and information sharing of phishing websites and suspected fraudulent malicious programs, take action on phishing websites and fraudulent malicious programs in a timely manner according to law, and promptly remind the masses of fraudulent phishing websites and malicious programs.
In accordance with the monitoring data, F detected a total of 1,030 tampered government websites in China in 2020, an increase of 30.9% compared with the number in the same period in 2019 (787).

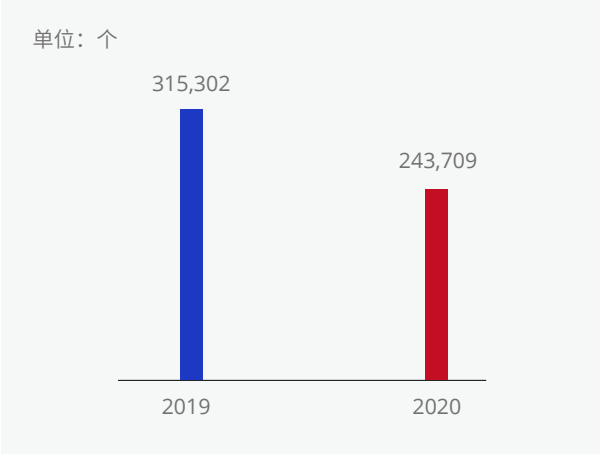


Figure 77: number of tampered websites in China

Common digital risks for government:

Brand infringement

Data breach

7.2.7 Universities and Colleges

Every year, with the launch of college admissions across China, some criminals begin to take educational institution websites and websites for score inquiry, admission application, and studying abroad consultation etc. as new phishing targets. According to a responsible official in charge of the Secretariat of the China Anti-

Phishing Website Alliance, based on the characteristics of educational phishing websites in previous years, there may be three common fraudulent methods. The first, phishing websites are made in accordance with regular college websites and online application systems as counterfeit objects. Then, the production and dissemination of phishing websites target for personal sensitive information. And websites of colleges and universities which do not exist are created.

The “Copycat Colleges” such as “Guangzhou Institute of Technology” and “Normal University of North China”, disclosed by the media, stole the teachers’ profiles from other regular college websites. The “Admission Brochures”, which was randomly patched up, even boldly printed clone college logo on the front page. Such fake websites with genuine and fake information together made it difficult for students and parents to distinguish. At the same time, the responsible official indicated that the websites of regular colleges and universities did not pay much attention to the establishment of monitoring mechanism for fake and phishing websites, which provided criminals with a great opportunity to make ill-gotten money. Fake websites not only seriously damaged the interests of parents and students, but also undermined the image of regular colleges and universities. , and disrupted the online academic order.

In addition to the fake admissions above-mentioned, phishing websites imitating colleges and universities are often used to diverse traffic for illegal activities. From the appearance, many counterfeit websites are roughly the same as the official organization websites, but they actually promote advertisements related to pornography, gambling or other illegal activities on a certain page. Viewers may be misled to illegal websites, resulting in the leakage of money or sensitive information. This act seriously affects the reputation of higher education institutions and damages the positive image of China's education in the hearts of the masses.

Figure 78: football lottery fishing website of a well-known university

With the improvement of financial capacity, more and more students choose to study abroad. The United States, the United Kingdom, Canada, Australia, etc. are all popular choices. In April 2021, CCTV Finance reported that the number of applicants for studying abroad for undergraduates, masters and PhDs had surged by 50% this year, hitting a record high. It is such a huge potential market that a large number of international criminals extend their black hands to the international students.

Although today's technology is increasingly developed, we can easily have access to foreign universities, but the information obtained is fragmented and mixed with false messages. For students who are not very familiar with the application process for studying abroad, especially the parents who are not used to English language, it is too difficult to identify and filter out the information that is really beneficial to them. In such a sophisticated environment, many lawbreakers grab their own "business opportunities". They create all kinds of phishing websites that imitate foreign official websites, and steal money or sensitive information by some

specific means.

The BBC once exposed a case where the official website of a British university was counterfeited by criminals who emailed to international students to steal their tuition fees. There are two main types of scams of the phishing website. The first is to directly charge students when they register and apply for online courses. The second is to collect the application students' personal information, such as passport number, mobile phone number, full name, date of birth, credit card, etc., for subsequent fraud activities. It is worth mentioning that, no matter what kind, once fooled, the possibility of recovering the loss is very low.

Figure 79: Phishing website of a famous British university

After the case was exposed by the media, although the university involved clarified its relationship with the phishing website on social media, but the damage was real and the public blamed the university for lack of regulation. What is more, it is difficult to ensure that other universities do not have similar phishing websites on the Internet. In order to prevent their legitimate rights and interests from being damaged, international students should improve their awareness. And on the other hand, it is also necessary for universities to monitor infringing websites that damage their own reputation.

Common digital risks in the universities and colleges:

Brand infringement

Data breach

7.2.8 Foreign-funded Institutions

Since the implementation of Chinese economic reform, the investment scale of foreign-funded enterprises has increased from small to large, capacity from low to high, and location from coastal areas to island areas. In the progress of China's magnificent prosperity, foreign-invested enterprises have always been important participants, witnesses, and beneficiaries. And China will still be an ideal destination for multinational companies to invest in in the future. By 2021, foreign enterprises have set foot in various industries such as finance, securities, insurance, catering, hotels, retail, logistics, e-commerce, services, and investment in China. Although foreign companies are numerous and complex, most of them experience the same predicament when digital risks come.

Most of the foreign companies entering the Chinese market are world-renowned international brands, which have already established a good reputation and won consumers compliments. Criminals value and use their influence on consumers to create a large number of phishing websites imitating legitimate ones to steal money and sensitive information. Many people relax their vigilance because of their trust in the brand, but unfortunately exploited by scammers.

In addition, even if phishing or infringement occurs, foreign enterprises may not respond to risks in a timely

manner for being not familiar with Chinese laws and regulations. Furthermore, during the takedown period, more harms may be created to possible victims.

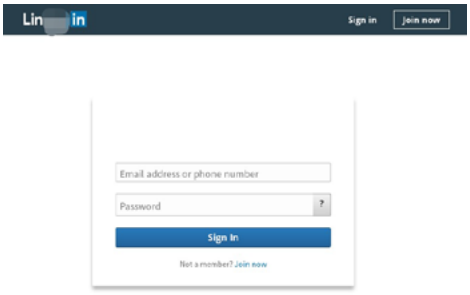


Figure 80: phishing website of a well-known American social media

Figure 81: phishing website of a large US logistics company

Common digital risks for foreign companies:

Phishing Fraud

Brand infringement

Data breach

7.2.9 Medical Institutions and Health Care

With the advent of the 5G era, personalized medicine, remote diagnosis, and remote treatment have gradually entered people's lives. All of this is based on the huge amount of health and medical big data information, which has become a national basic strategic resource. China is deeply aware of the importance of big data in health care. Promoting the national application of big data in health care is dedicated to seize the forefront of innovative medical research, precise diagnosis, personalized health management and mobile medicine. However, with the increasing scale of medical big data, the data security issues are also increasingly prominent. More and more data is being sold openly through various channels. The medical industry is related to the national economy and people's livelihood. Once medical data is tampered with, destroyed or leaked, it will inevitably trigger a serious threat to the reputation of medical institutions, the privacy and health safety of both doctors and patients, and even affecting the social harmony and stability.

In accordance with Cost of a Data Breach Report 2021 released by IBM, the average cost of a global medical data breach in 2021 is as high as $9.23 million , an increase of 29.5%. And the cost of data breaches in the healthcare industry ranks the highest for 11 consecutive years. The healthcare industry saw a 58% increase in confirmed data breaches in 2020. More than 93% of healthcare organizations experienced a data breach between 2018 and mid-2020. It can be seen that the medical industry is deeply poisoned by data leakage.

Figure 82: During the pandemic, a hospital in Jiaozhou leaked medical records of patients and their families

In addition to data breaches, phishing behaviors targeting the medical industry are not uncommon. A vaccine manufacturing company has become a popular impersonation target for phishing attackers. According to a new report from INKY, a phishing email campaign that began around August 15, 2021 impersonated the company in an attempt to steal business and financial information from victims. The perpetrators purchased several anonymous domain names highly similar to official websites and registering e-mail services to steal confidential business information by sending recipients emails on topics such as urgent offers, tenders and industrial equipment supply.

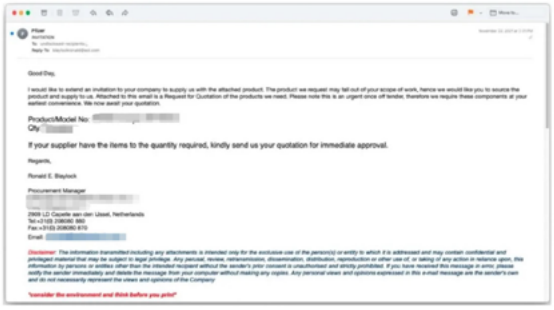


Figure 83: email imitating a vaccine company

Common digital risks for medical institutions and health care:

Data breach

Phishing Fraud

Brand infringement

7.2.10 E-commerce and Digital Enterprise

In recent years, the development of the Internet industry in China is blooming, which not only drives economic development, but also effectively triggers the upgrading of Chinese industrial structure. Leading enterprises such as Alibaba, Tencent, and Meituan contribute to digital technological innovation. Then a group of small and medium-sized Internet companies have risen to devote to the industry. Today, these Internet companies have penetrated into the necessities of life of the common people, providing with the best quality services.

From social media to retail, internet brands are using more and more touch points to interact with consumers. The safety degree of consumers at touch points will become an important difference for competitiveness on the market. The security of these touch points guarantees the basic consumers safety at every step of the interaction with the brand. Therefore, the demand for digital risk protection by Internet companies is increasing day by day .

The difficulty for Internet companies to protect their digital assets stems from the huge assets volume, which is closely related to the lives of the people, the complex types of digital risks, and the limited size of the internal security teams. The protection effect only relying on manual monitoring is minimal. On the other hand, digital risks can also evolve over time to evade detection. All of this exhausts security personnel in the response progress.

There are many types of digital risks for Internet companies, but they mainly focus on three categories:

website phishing and counterfeiting, brand infringement and APP counterfeiting.

Figure 84: a counterfeit APP of a well-known Internet company

Figure 85: a phishing website of a well-known Internet company

Figure 86: a website of trademark infringement of a well-known Internet company

Common digital risks for e-commerce and digital companies:

Phishing scam

Brand infringement

APP counterfeiting

Social Media Phishing

Data breach

7.2.11 Online Gaming

In past few years, video games, as entertainment consuming products, have now become a very important part of the entertainment industry with the increasingly powerful network economy. Newzoo forecasted total video game industry revenue of $175.8 billion in 2021, slightly lower than 2020's, but still significantly higher than the figures before the pandemic. The reason why the virtual game world is welcomed is mainly because games not only provide opportunities for relaxation, but are also endowed with opportunities of social activities with strangers. There are currently 2.7 billion gamers worldwide. And mobile games in particular are attracting more and more users. This rapid growth is due to the increasing amount of mobile games and the focus on social interaction during the COVID-19.

However, just as the game industry is in prosperity, in August 2021 Kaspersky released the "Analytical report on gaming-related cyberthreats in 2020-2021". The report showed that attacks on PC and mobile gamers were also growing rapidly with the gaming industry's revenue. From July 1, 2020 to June 30, 2021, the total number of users who encountered game-related malware and malicious software (or unwanted software) was 303,827. Among them, a total of 50,644 users tried to download 10,488 malicious phishing apps disguised as top ten popular mobile games, and detected 332,570 times overall.

Furthermore, 83% of the mobile games with threats were due to the APP adware insert, affecting a total of 48,492 users. While adware is not malicious, illegal ads can ruin the quality of the user experience and put user data at risk. Besides, because of its highly intrusive feature, adware often renders mobile devices unusable. Similar apps may be listed on third-party app stores without official authorization from legitimate brand owner. And the app stores do not conduct any technical inspections on the apps launched.

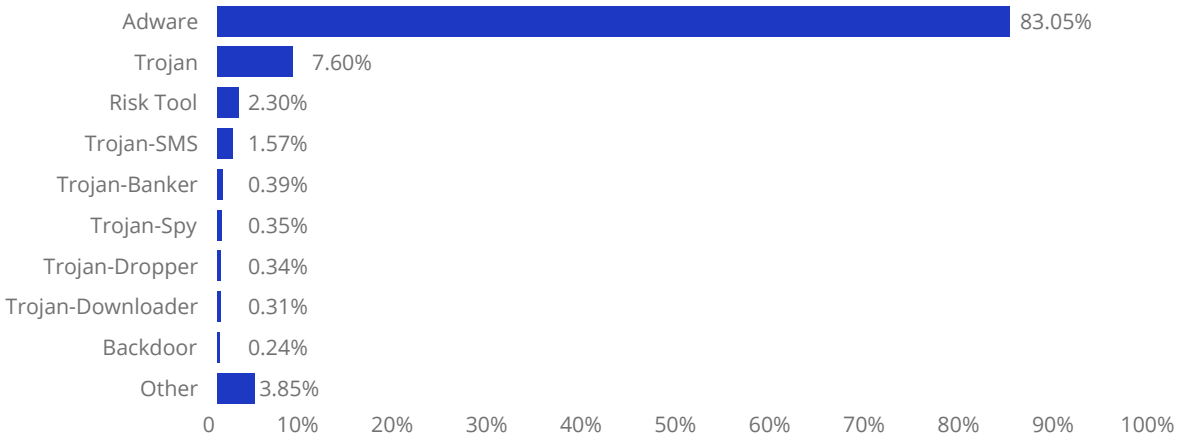


Figure 87: types of threats in game apps

In addition to adware, the research also detected a number of dangerous malware, such as personal information and bank account stealing tools, often causing users to lose account credentials and lose money (including cryptocurrencies).

Common digital risks in the gaming industry:

APP counterfeiting

Phishing Fraud

Data breach

Brand infringement

7.3 Digital Risk Awareness Management

Just as risk awareness is an important part of cyber security management, digital risk awareness determines an enterprise's attitude to digital risk management and is the source of digital risk protection. Marketing, legal affairs, risk control, human resources, finance, executives, technical teams, etc., may all be potential targets of digital risks. Therefore, cultivating the risk awareness of personnel is an indispensable part of the digital risk protection system. Digital risk awareness management can start from the following aspects.

7.3.1 Establishment of Dedicated Teams

In the work of digital risk protection, the first task is to set up a dedicated team with members from multiple departments including IT, legal, finance, and business. The team should clarify the strategies for digital risk protection, and implement relevant responsibilities, and ensure that the protection work can be carried out in a long term.

7.3.2 Online Awareness Education

Use corporate websites, APPs, official accounts and other channels to propagate network security culture and relevant laws. At the same time, online education is provided to employees to enhance awareness of security and confidentiality through course study, self-assessment exams, game competitions, active notification and other methods.

7.3.3 On-site Professional Training

Professional training lecturers hold on-site lectures and demonstrate various social engineering attacks or fraud techniques to enhance personnel's security awareness.

7.4 Establishing a Complete Digital Risk Protection Mechanism

According to the IDRR framework, enterprises can establish a complete digital risk protection mechanism.

7.4.1 Identifying Digital Assets(Phase I)

It is crucial for enterprise to identify valuable digital assets, evaluate the footprint and assets exposure, analyze possible digital risks and losses, and formulate protection strategies with purposes. The digital assets of enterprises include but not limited to official domain names, mobile apps, social media accounts, enterprise data, copyright documents, core codes, and search engine rankings.

7.4.2 Real-time Risks Monitoring and Detection(Phase D)

For brands or target assets, continuous online monitoring needs to be implemented to identify network security incidents and abnormal activities, and assess the risk level, and ensure the comprehensiveness of the monitoring scope, the rapidity and accuracy of monitoring results.

7.4.3 Comprehensive Alarming Mechanism(R1 stage)

For the risk discovered, there are various alarm methods such as email, SMS, WeChat, and telephone to ensure that the responsible staff knows the risk situation at the first time, so as to implement the response mechanism in time, eliminate the impact of the event, and prevent the spread of the impact.

7.4.4 Fast Takedown(R1 stage)

For all kinds of risks faced by confirmed digital assets, regardless of risk location, rapid takedown can be implemented to alleviate or eliminate the risk impact. On the other hand, it is essential to collect sufficient evidences for appeal application and a complete authorization chain to ensure the legitimacy and completeness of the disposal operation itself.

7.4.5 Continuous Monitoring(R2 stage)

Fraud or infringing groups often adjust their strategies and conduct continuous confrontation after being counter-attacked. For digital risks that have been dealt with, continuous tracking and monitoring need to be carried out. If a risk of "resurrection" occurs, the response mechanism can be restarted immediately to ensure the complete elimination of risks.

7.4.6 In-depth Risk Analysis(R2 stage)

The monitored data are ready to be aggregated for in-depth analysis reports which are generated from various dimensions. As for the lessons learned, monitoring and takedown experience can be incorporated into improvement plans. Active detection and defence should integrate digital risk protection into daily cyber security protection progress.

7.5 Evaluation of Digital Risk Protection Outsourcing Services

Since digital risks are mainly distributed outside the enterprise's protection range, technical and management challenges are raised at all stages of protection. In order to reduce the cost of dealing with digital risks, companies usually adopt the outsourcing protection services. Therefore, the evaluation of service providers is also very important. Usually, the following comprehensive factors can be considered when external service providers are needed.

7.5.1 Global Capacity Coverage

Mature service providers are required to establish a global digital risk monitoring system through technologies such as threat intelligence exchange, newly registered domain name monitoring, and active detection, etc. Phishing, and infringing attackers are distributed globally. Mature service providers are capable of communicating and cooperating with network service providers over the world. No matter where the malicious criminal hides, the risk subject can be quickly shut down.

7.5.2 Comprehensive Use Cases

According to the customers different requirements toward various use cases, the service scope of mature external service providers can cover various online platforms, such as websites, App stores, social media, online storage, knowledge communities, deep web and dark web, etc. Comprehensive digital risk use cases are preferable, including but not limited to phishing fraud, brand infringement, data leakage, copyright piracy, false positive, malicious search engine rankings, etc.

7.5.3 Mature Strategies

Mature external service providers have systematic coping strategies. In-depth analysis technologies such as machine learning, natural semantic processing, and data mining can be used to provide users with continuous risk traceability. Multilingual communication skills are required. It is compulsory to be familiar with the takedown process on different platforms and legal service systems around the world.

7.5.4 Fast Takedown

Digital risk are often highly time-sensitive. Mature external service providers need to respond in the shortest time to eliminate various risks, restore brand reputation, and protect business value. The takedown capacity should maintain the leading position in the industry over the world.

7.5.5 Service Impact

Mature external service providers can offer timely, efficient and high-quality services to customers across the country. It can realize 7*24 hours real-time monitoring and response, and alert customers through email, SMS, WeChat and other methods. The takedown is carried out with global coverage. Under the premise of sufficient evidence, the takedown success rate exceeds 95%, and with standard delivery SLA specifications. In-depth risk analysis reports help customers improve emergency response mechanism.

7.6 Digital Risk Challenges of Chinese Enterprises

7.6.1 Cross-border Origination

For digital risks targeting Chinese companies and their users, criminals often deploy servers and other resources outside the Chinese territory in order to evade supervision and police fighting This increases the difficulty of implementation for risk discovery and elimination.

7.6.2 Time Sensitivity

Digital risks are often urgent and time-sensitive when they occur. Once the best time to solve the problem is missed, the loss of the enterprise will not be recovered in time, but may be extended.

Moreover, as for online attacks, the transfer speed of the hosting subject is very fast, which is difficult to fight back with traditional means.

7.6.3 Language Barrier

As digital risks are all over the world, risk resolution requires companies to communicate with various service providers, major social media platforms, and regulatory agencies around the world. This requires a very high cost of time and energy for enterprises.

7.6.4 Global Digital Assets Protection

With the continuous improvement of business capability, more and more domestic enterprises who have the requirements to "go overseas", may encounter numerous digital risks during the journey. However, most enterprises are not familiar with the foreign language environment, and hesitate in the stage of identifying their own risks, let alone risks coping.

7.7 Digital Risk Challenges for Multinational Corporations in China

7.7.1 Culture and Language Challenge

After entering the Chinese market, foreign corporations may also face countless digital risks due to their brand reputation However, most companies are not familiar with the Chinese language environment, and the rapid changes in Chinese domestic industrial condition have brought great challenges to foreign companies in identifying their own risks.

7.7.2 Local Regulation Challenge

The laws of different countries and regions usually vary greatly. After landing in China, foreign corporations fail to take proper protection measures when encountering digital risks, due to being unfamiliar with Chinese legal system and regulations, which seriously hinders their business promotion and brand building.

7.7.3 Incident Response Challenge

Facing digital risks occurring in China, foreign corporation usually lack mature and systematic response strategies. The risk verification rules of domestic mainstream service providers and social media platforms are different. And the work habits of domestic companies and foreign ones are also quite distinct. The above

mentioned results in inefficient communication, long takedown time, and low takedown success rate.

08 Summary

In the Internet age, more and more institutions, enterprises and individuals are aware of the importance of digital risk protection, paying more and more attention to maintaining digital assets and brand image, as well as the hidden value behind.

However, out of the openness of the digital risks mentioned in this article, there are many difficulties in the early-aged protection measures. The response can only be initiated from the incident occurrence. Many corporations are inexperienced, and often caught in the dilemma of what to do, which misses the best time to solve problems.

Tianji Partners recommends the IDRR model be adopted, and taking compliance and business requirements as the penetration point for digital risk sorting, establishing a complete emergency response mechanism, and at the same time providing employee with security awareness training, selecting outstanding digital risk partners, and integrating digital risk protection into daily work.

天际友盟
TianJi Partners

Digital Risk Protection Specialist

400-081-0700 www.tj-un.com www.twitter.com/TianJiPartners

Market cooperation：mkt@tj-un.com Customer service：service@tj-un.com Partner：partner@tj-un.com