Technical Specification

ISO/TS 22386

First edition
2024-10

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for brand protection and enforcement procedures

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices pour la protection des marques et les procédures de mise en application

ISO/TS 22386:2024(en)

COPYRIGHT PROTECTED DOCUMENT

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The value of brands to a brand owner is both intangible and tangible. Brands are built as part of the intellectual property rights (IPR) of the brand owner and enhance its related innovations. Brand reputation relies on the brand owner's investment and often leads to brand equity, including consumer trust and confidence.

In recent years, counterfeiting activities have become increasingly aggressive, causing harm to brands. Besides damages to a brand owner's intangible and tangible assets, such activities also pose a threat to the global economy and critical infrastructure assets, while endangering consumer health and safety. Those responsible for counterfeiting products are solely seeking self-benefit, which means that they are likely to provide poor working conditions, use child labour, contribute to human trafficking and criminal organizations. They also do not invest in research and design; instead, they exist by plagiarizing others' creations and innovations. This harms the entire IPR intensive industry.

NOTE   For more information on IPR intensive industry, see EPO/EUIPO (October 2022), IPR-intensive industries and economic performance in the European Union Industry-level analysis report, fourth edition October 2022. [17]

Counterfeiting activities also have a negative environmental impact during and after the manufacturing of counterfeit goods, such as the release of toxic waste into the environment.

Brand protection activities, therefore, are meaningful. By the protection of brands and their related brand reputation/image, sales and revenues are increased, IP assets are also protected, and their consumers' benefits are ultimately protected.

Therefore, brand owners can utilize this document to make their brand protection activities efficient, effective, professional and valuable. This document is designed to provide guidelines for brand protection activities, aiming to build a unified terminology and set of activity elements.

Online enforcement is becoming an increasingly important element in brand protection. However, online enforcement is not detailed in this document and will be left for future development.

The following relevant international standards can be used in conjunction with this document.

— ISO 9004, which gives guidelines for enhancing an organization's ability to achieve sustained success.

— ISO 31000, which provides principles, a framework and a process for managing risk.

— ISO 22384, which sets up a process to assess risks, and to select and combine individual measures for developing a product protection plan. It includes consideration of impacts and modifications to, for example, product lifecycle, supply chain, manufacturing, data management, brand perception and costs so as to adapt the protection plan accordingly.

— ISO 28000, which specifies requirements for a security management system, including aspects relevant to the supply chain.

— ISO 22380, which provides guidance on how organizations can establish strategic, business countermeasures to prevent or reduce any harm, tangible or intangible loss and cost from such fraudulent attacks in a cost-effective manner.

— ISO 22383, which gives guidelines for performance criteria and an evaluation methodology for authentication solutions that aim to unambiguously establish material good authenticity and integrity throughout an entire material good's lifecycle.

— ISO 22378, which describes framework for identification and authentication systems.

— ISO/IEC 27001, which provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

— ISO 31700-1, which establishes high-level requirements for privacy by design to protect privacy throughout the lifecycle of a consumer product, including data processed by the consumer.

— ISO/TR 31700-2, which provides illustrative use cases, with associated analysis, chosen to assist in understanding the requirements of ISO 31700-1.

This document provides guidance for professionals within brand protection including, but not limited to:

— a management team of brand owners

— brand protection managers and practitioners

— IP and trademark attorneys

— investigators

— online monitoring solution providers

— authentication solution providers

— business intelligence and data analysts

— inspection and enforcement authorities

— associations for brand protection

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for brand protection and enforcement procedures

1 Scope

This document provides guidelines for establishing and enforcing respective measures for brand protection. It supports the development of a brand protection strategy and describes a brand protection framework for the development, production, and distribution of products and documents.

Applying these guidelines throughout the product lifecycle can facilitate interaction between individuals and organizations involved in brand protection activities and can make brand protection procedures more effective and efficient.

This document is intended to support the brand owner's business resilience, brand reputation, and brand value, by protecting products, documents, and associated services from counterfeiting and other infringements.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 General terms related to brand protection

3.1.1
anti-counterfeiting
process of either combating counterfeiting activities or counterfeit products, or both

3.1.2
brand protection
process of either protecting brands against counterfeiting or other infringement acts, or both

3.1.3
brand protection activity
event undertaken by a right owner (or on its behalf) for the purpose of *brand protection* (3.1.2)

3.1.4
case
series of events or persons being dealt with by *brand protection* (3.1.2) teams

3.1.5
customs training
training provided to customs authorities for the learning and development of knowledge, skills and abilities, of the intellectual property rights and products of a specific company or companies

3.1.6
genuine product
product that is manufactured by, or authorized to be manufactured by, the brand owner, used as reference for identifying suspect counterfeit products

3.1.7
infringing product
product that is made without licensing or authorization

3.1.8
intellectual property
IP
output of creative human thought process that has some intellectual or informational value

[SOURCE: ISO/IEC/IEEE 26511:2018, 3.1.19]

3.1.9
intellectual property infringement
unauthorized use, reproduction, distribution, or violation of *intellectual property* (3.1.8) rights

3.1.10
intellectual property portfolio
collection of *intellectual property* (3.1.8) rights owned by one entity

3.1.11
key performance indicator
KPI
quantifiable measure that an organization uses to gauge or compare performance in terms of meeting its strategic and operational objectives

3.1.12
product identification
product verification
product authentication
process to determine whether a product is counterfeit or not

3.1.13
return on investment
ROI
measure of performance represented in the form of a ratio calculated by the benefit of an investment divided by the cost of an investment, which is used to evaluate the profitability of an investment

3.2 Terms related to organization and individuals

3.2.1
brand protection manager
individual who is responsible for strategizing, planning, conducting and evaluating *brand protection activities* (3.1.3)

3.2.2
infringer
individual or company who has infringed the *intellectual property* (3.1.8) rights of third parties

3.2.3
leads
source of information that can lead to *brand protection activities* (3.1.3)

3.2.4
online marketplace
e-commerce site where multiple *parties* (3.2.6) advertise and sell their products/services

3.2.5
party
person or group related to a *brand protection* (3.1.2) case, who is concerned with or affected by the activities of a *case* (3.1.4)

3.2.6
product expert
individual who has expertise on the products of a company, and can provide knowledge in the identification of counterfeit products

3.2.7
suspect
individual or company whose history or any other information leads to a suspicion that it can be an *infringer* (3.2.3) to *intellectual property* (3.1.8) rights

3.3   Terms related to enforcement

3.3.1
customs recordal
application for action
registration of the *intellectual property* (3.1.8) rights with customs authorities that allows customs to monitor shipments and exclude, detain or seize goods that are suspected of being counterfeit or infringing the recorded intellectual property rights

3.3.2
cease and desist letter
C and D letter
request sent to an individual or company to stop an activity ("cease") and refrain from doing it again ("desist")

3.3.3
ex officio
procedure for carrying out customs controls, whereby customs can come across goods that can be infringing rights but for which no *application for action* (3.3.1) has been submitted

Note 1 to entry: Customs can also suspend the release of these goods, or detain them.

3.3.4
market sweep
action or process to take down counterfeiting products or online product listings in one market at one time

3.3.5
raid
action to seize all infringing items and collect evidence on location

3.3.6
settlement
agreement between the infringed and infringing parties without depending on a court decision or other enforcement actions

3.3.7
test purchase
buying products from a suspect shop anonymously so as to identify the products, and to collect information and evidence about the suspected counterfeiting activities

3.4 Terms related to case management and intelligence

3.4.1
application programming interface
API
collection of invocation methods and associated parameters used by one piece of software to request actions from another piece of software

[SOURCE: ISO/IEC 18012-1:2004, 3.1.1]

3.4.2
case management
management of *cases* (3.1.4) and their related tasks, workflows, documents, reports and statistics, etc.

3.4.3
case management system
software system that supports the management of *cases* (3.1.4) and their related tasks, workflows, documents, reports and statistics, etc.

3.4.4
product library
library of products of brand owners, which are used as reference for identifying suspect counterfeiting products

3.4.5
heat map
display of geographical coverage of suspects/infringements that depicts the areas on which *brand protection activities* (3.1.3) focus

3.4.6
data analytics
composite concept consisting of data acquisition, data collection, data validation, data processing, including data quantification, data visualization, and data interpretation

[SOURCE: ISO/IEC 20546:2019, 3.1.6]

3.5 List of abbreviated terms

API   application programming interface

BI   business intelligence

IP   intellectual property

IPR   intellectual property rights

KPI   key performance indicator

ROI   return on investment

4 Foundation of brand protection — IP portfolio

IPR registration provides a legal basis for the protection of a brand. The relevant IPR can be in particular:

— Trademark

— Design

— Copyright

— Patent

— Domain name

— Trade name

— Utility patent

A broad IP portfolio helps to enhance and expand the company's brand protection. Broad coverage for the IP rights related to the brand should be acquired within a reasonable budget.

A brand owner should identify the elements eligible for IP protection and identify those that are of the most value. This includes obtaining IP rights that provide the most beneficial, sustainable and long-term protection.

The brand owner should identify the IP that has suffered the most infringements. A large amount of infringement causes huge damages, and thus registration for such IP rights would serve as a basis for legal action to mitigate potential damages.

The brand owner should determine markets, regions, or countries where counterfeiting activities are most prevalent or cause the most damage. The brand owner should establish exclusive and comprehensive coverage by securing a wide class of goods and services for the IP rights in those regions/countries.

The brand owner should consider market forces, such as:

— Market regions and countries, especially where the products have a competitive edge; IP rights to be protected in the locations where the products are sold.

— Products that are most commonly infringed/counterfeited. Such products should be covered with IP rights.

— Enforcement ease (refer to the effort required to demonstrate the counterfeit character of a product and, the validity of the legal basis).

— Alignment between IP rights with business goals.

— Legislative and enforcement procedures in different regions and countries.

— The legal framework of the country where the most infringements occur or where damages are the highest.

— Costs (for registration, IP procedures, and maintenance).

— Time limitation of IP rights versus a lifetime of the product.

— IPR that should be registered and applied before the products are put on the market.

5   Objectives for brand protection activities

5.1   Set the goals

The brand owner should consider the following aspects to ensure the appropriate protection of the brand:

— safeguarding the safety of consumers and patients;

— safeguarding the brand's reputation;

— safeguarding the integrity of the product, including its packaging;

— ensuring freedom of operation, i.e. by not infringing another party's IP rights;

— enforcing its own IP rights against infringement;

— ensuring the authorized use of trademark in accordance with the right holder's guidelines;

— supporting sales and after-sales activities;

— supporting dealer network management and supply chain management;

— protecting substantial revenue through law enforcement activities.

Depending on the different stages of the business and the industry, the goal of brand protection activities can be reactive actions or preventive actions. It can cover the entire product lifecycle. The brand owner should truly understand the actual business needs before setting the goals.

5.2 Common challenges

This subclause presents the role of brand protection activities for handling the most common challenges that businesses can face. Some of the commonly encountered challenges include the following:

— Market share is or will be taken by a counterfeit product sold online or in physical stores offline.

— A product is copied before the official release.

— Consumers cannot differentiate between genuine and counterfeit products.

— Internal employees cannot distinguish between genuine and counterfeit products.

— Facing a large number of consumer complaints about counterfeit products on the market.

— Consumers knowingly buy counterfeit products.

— Consumers associate low-quality counterfeit products with genuine products.

— Genuine products in the market can infringe other party's IP rights.

— The research and development/design department lacks a process for evaluating other party's IP rights.

— The research and development/design department lacks have a process for following company brand guidelines.

— Dealers or distributors are unaware of or ignore company brand guidelines within the authorized scope.

— Dealers or distributors misuse the brand outside the authorized scope.

— End consumer/client suffers from damages due to counterfeit products.

— The infringer forges the brand owner's identity to conduct illegal business.

— Illegitimate reuse of packaging materials such as bottles, disposed products, etc.

5.3 Prioritization and integration

The brand owners can be aware of, or can have encountered, most of the scenarios specified in 5.2. However, it is still an important question of how to prioritize them. Brand protection teams can be easily flooded with thousands of interesting potential leads or pieces of information from both external and internal sources but end up with nothing being conclusive. The brand owner should prioritize the known challenges. This ensures that everyone in the brand protection team cooperates with each other and aims towards the same direction.

In most multinational organizations, brand protection teams are not always the closest to the business, but still must meet the expectations of the business and support company goals. As the first step in setting goals, after identifying all stakeholders, brand protection teams should find all possible ways to fully understand the company strategy. This information will not come solely from the department head. It is essential to also identify the links and dependencies between departments in order to understand other departments' goals. Special consideration should be given to supporting of and collaborating with the marketing, sales, aftersales, and research and development/design departments.

As a second step, it is recommended to make a list of all the needs and challenges specific to each department. Examination of this information can provide insight into why the issues exist and potential causal links between issues. This work can then guide brand protection efforts to contribute to their resolution.

As a third step, if budget allows, conducting key market research is another way to verify if the known information is still up to date and accurate, especially when there are no local partners to support the information collection.

As a last step, prioritize the list by considering the importance and urgency of each potential goal. This can be achieved by considering the following:

— If this challenge is solved, how much will it contribute to reaching the company strategy? This enables the "importance" to be determined.

— If this topic is strongly connected to consumer safety, current sales targets, or high-risk lawsuits, then it is absolutely urgent.

Using a 5-level ranking system, such as "very high, high, medium, low, very low" should be sufficient to illustrate the final prioritization in a simple way. In the end, the ranking results will show which goal is the most important to be attended to first, before the other goals are attended to.

5.4   Return on investment (ROI) considerations

The brand owner should calculate the ROI calculations by dividing the net benefit by the cost of the investment. The measurements include both hard ROI indicators, i.e. indicators that tend to be easy to quantify, and soft ROI indicators, i.e. indicators that are intangible, such as brand reputation or consumer awareness. Brand protection teams can interpret the value of seized counterfeit goods as the net benefit. The cost of investment can be the sum of internal and external costs of brand protection activities.

NOTE   Using the prevention value as the "net benefit" can be challenged by the business, on the grounds that the seized goods or removed listings are not necessarily equal to sold genuine goods.

Brand protection is not only about preventing losses and damages. The brand owner should consider generating recovery income as well. For example, when a civil litigation judgment is in favour of the brands, or a settlement is reached between the brand and the infringer, these should be directly calculated into net benefits.

As many brand protection teams may have already experienced, it is almost impossible to calculate a desired brand protection ROI in general. Instead, it would be more feasible to set up specific evaluation methods for specific enforcement activities. Given that high priority goals usually require more attention and resources, it is worth investing additional effort in measuring them. Therefore, it makes sense to focus on improving the efficiency of utilizing resources and try to find what is "small but beautiful".

For example, many consumer brands that enforce their rights through customs action want to improve the ROI on this particular topic. This raises the following questions: "Do customs actually improve their performance after a brand's investment? Which customs brings the best result, which is the most active, and the most accurate in detaining goods that are also subsequently identified as counterfeit?"

To be able to answer these questions, the team needs a tool or system to collect case data and figures for statistical analytics. For example, among all customs cases in a specific time frame, it is important to determine the number of products are seized, the number of products released, and the costs of handling these cases. Then it becomes possible to calculate the costs and benefits, compare different countries, and analyse historical performance. This includes identifying products that are reported by customs but the majority of them are genuine. Only after being aware of those issues, it is possible to determine a goal for general and regional customs enforcement.

5.5   Measurement of key performance indicators (KPI)

The brand owner should use key performance indicators (KPI), objectives and key results (OKR), or similar methods to help measure the efficiency of brand protection activities and to achieve key business objectives.

It is recommended that the KPIs are measured in the following way:

— List the goals with the brand protection team.

— List the possible measures to reach those goals, these are the KPIs to measure brand protection activity effectiveness.

— Set a plan for enforcing these goals that will be directly related to the brand protection team's performance.

— Let the brand protection team takes responsibility for monitoring their own performance and reporting statistics.

Table 1 shows some examples of brand protection KPI metrics.

Table 1 — Common brand protection goals and associated metrics

Goals	Metrics	Resources	Responsible
Customs seizure	Number of customs trainings, seizure quantity and seizure values	Law enforcement authorities, law firms	Regional brand protection managers
Online monitoring	Web monitoring solution implementation, delisting success rate, amount of take-downs	Online monitoring software and service provider	Core team
Market control	Number and types of customer complaints; number of raids, investigation, market survey	Internal departments and external service providers	Regional brand protection managers
Internal security	Improved product identification solution, implementation of security labels, internal audit on supply chain and distribution channel	Internal departments and external service providers	Brand protection team
Team management	Workflow, intelligence sharing, communication efficiency, statistic, report	Consulting service provider and case management software	Brand protection team

5.6 Managing risks

The brand owner should ensure the management of risks and issues that are detrimental to brand protection goals by:

— establishing the context;

— assessing, treating, monitoring, reviewing, recording, and reporting;

— communicating and discussing the risks.

Appropriate risk assessment should be conducted for each goal to determine how it can be impacted by a risk event. Risk assessment includes risk identification, risk analysis, and risk evaluation. Each planned action to mitigate risks should be monitored, reviewed, reported, and communicated by the brand protection team. These risks can impact the achievement of goals.

6 Building a brand protection team

6.1 Team expertise

The brand owner should set up a brand protection team with the relevant expertise.

The brand protection team should consist of members with the following expertise:

— Team manager

— IP specialist

— Legal counsel

— Security specialist

— Product expert who can distinguish between genuine and counterfeit products

— Experts who provide input and expertise throughout the product lifecycle

The team should be engaged in new product development, potential retrofitting existing products, as well as the assessment of technologies that best fit the product design and intended markets. A robust product design with layered techniques utilizing covert or overt technologies (or both) will inherently reduce counterfeiting, enhance the market detections of counterfeit products and improve enforcement activities.

Brand protection team members perform all the daily operations related to counterfeiting cases including assigning tasks, test purchases, interacting with external counsel, web monitoring, investigating, as well as liaison with law enforcement authorities. They also help to enforce actions against the counterfeiters.

6.2 Members roles

The brand protection team should consist of members who can handle multi-functional tasks and multiple projects at the same time. The different roles they play can include:

— Team leader, who is responsible for leading the internal brand protection team or service provider to reach the goals, setting up strategies, recruitment and allocation of human resources and budget, and delivery of status/issues/progress reports to corporate management. The team leader should be experienced in brand protection procedures and have knowledge about the brand owner's products, industry, and organization.

— Investigator, who is responsible for gathering intelligence and carrying out investigations against those who infringe intellectual property rights and other related interests.

— Legal counsel, who possesses a legal background, provides legal opinions and performs tasks related not only to Intellectual Property law but also to other legal matters such as civil proceedings and criminal proceedings.

— IP specialist, who is in charge of application, opposition, and renewal of trademark, patents and other IP rights, provides internal knowledge about the brand owner's current portfolio and future IP strategy.

— Product expert, who acquires the resources and knowledge about how to distinguish between genuine and counterfeit products. The individual in this role should be capable of serving as an expert witness in court cases or providing affidavit evidence.

6.3 External resources and partners

When an in-house brand protection team takes the responsibility of setting the goals and strategy, as well as coordinating global brand protection activities, external resources can greatly assist in providing professional advice or handling local actions. The following external resources can be engaged from time to time by the brand owner:

— Law firm, which works with one or several brands; can be the contact point for local law enforcement authorities, customs; prepares anti-counterfeit investigations; and takes legal actions. An in-house team can partner with a law firm to serve as global counsel for running global IP profile and coordinating enforcement actions in different countries, and also keep communication with local law firms or service providers. The in-house team can also give instructions directly to local law firms.

— Investigator, who investigates and registers suspected counterfeit cases for clients. Investigators can handle test purchases, market surveys or field investigations, help with identification of counterfeiters in targeted markets, and collect evidence to arrange further actions, such as raids or lawsuits.

— Online-monitoring service provider, who provides its software solution and services; and detects and removes IP infringements, unauthorized listings from marketplaces, websites, social media and domains.

— Anti-counterfeit alliance, which is an industry association that combines the forces of multiple brand owners who share similar brand protection issues and provides enforcement solutions.

— Data and other software service provider. The brand protection team is advised to research available data providers that can be used to facilitate investigation or intelligence analyses. For example, global shipments via customs are public information that is available on a number of platforms with search and ranking functionalities. The case management solution, IP search, and portfolio management solution provide unique features that make brand protection work much more efficient and data-driven.

— Certification bodies that have authorized the use of their marks on the brand owner's products.

7 Brand protection strategy setup

7.1 Company alignment

Before setting a brand protection strategy, the brand protection strategy should be aligned with the overall company strategy and that of connecting various departments. The team should collaborate with other departments and work together toward a common goal.

7.2 Interrelation aspects

7.2.1 Sales department

The brand protection team should work closely with the sales department. The following aspects should be considered for alignment:

— market priority, i.e. country or region priority, and consumer profile priority, especially paying additional attention to the new markets, most profitable market, most vulnerable market and most enforcement effective market.

— Product line structure that has or can have counterfeiting issue, i.e. including information about the product portfolio and its classification. This is essential for the reporting of the brand protection working results. The aligned product structure also makes it easier to find the right contact person when the brand protection team needs product-specific information.

— Sales figure. The brand protection team should understand the markets in various countries through sales figures, and if certain markets are growing or have difficulties. A country with high sales figures can also mean a country with relatively higher risk of IP infringement.

— Sales channels. Understanding the legitimate sales channels, as well as the grey market channels, in both the online and offline physical channels, including outlet channels, will help the team to identify unauthorized products and IP infringing products.

— Distribution channels. These should be regularly inspected to prevent potential counterfeiting activities and unauthorized sales. The brand protection team should collaborate with the dealer network department to gain a thorough understanding of their interests and sources of profit.

— Product priority. The brand protection team should collect a list from sales to fully comprehend which products are more important. This typically includes highly profitable products, newly released products, most counterfeited products, and most innovative products.

7.2.2 Product manager

The brand protection team should also build a close relationship with the product managers, particularly the product manager for products of high priority. Product managers are responsible for product identification for the brand protection team, implementing security measures, and training the team among other tasks. Similarly, the brand protection team can bring valuable feedback on the security features of products and offer insight into product prioritization based on counterfeiting activities in the markets.

7.2.3 IP department

The IP team is another essential partner that the brand protection team should engage. Establishing a comprehensive understanding of the company's IP coverage is the basic homework before developing strategies, as brand protection activities should be predominantly supported by IP rights. Large organizations can have a large and complex IP portfolio. In such situations, close collaboration between the IP team and the brand protection team can be used to combat infringement and counterfeiting.

7.2.4 Marketing department

The brand protection team should receive frequent updates from the marketing department as well. Especially, in local markets, the marketing team can provide knowledge in product identification.

7.2.5 Information security department

The brand protection team can engage with the information technology and cybercrime teams (also sometimes known as "Information Security" or "Infosec"). These teams should provide valuable insights into brand misuse, such as phishing attempts and customer scams. These teams can also have the internal expertise and external resources for monitoring brand abuse, such as, domain monitoring subscriptions or cybersecurity tools. Aligning the brand protection program with these teams should ensure that there is no duplication of internal or external efforts.

7.2.6 Other aspects

Other types of information, such as logistic routes, suppliers, packaging and labelling processes, and security procedures, should also be known to the brand protection team. By having the full picture, the brand protection team would be able to see the overall complexity of brand protection and identify where the focus should be placed. There is no suitable way to set up a strategy if the brand protection team does not understand their own organization and product.

8 Proactive actions and enforcement

8.1 Proactive actions

Proactive actions are taken before the enforcement actions for planning and preparing purposes. The following actions can be taken to protect the brand:

— Customs recordal

    The brand owner should apply for customs recordals and renew it on time, based on their IPR in the countries and regions wherever border control should take place. Besides the action carried out by customs based on an application for action, customs officials can also suspend the release of these goods, or detain them via an ex officio procedure.

— Online and offline monitoring

    The brand protection team is recommended to continuously conduct monitoring of various online spaces such as search engines, websites, online marketplaces, social media, domain registration. The offline monitoring includes physical locations, such as stores, markets, exhibitions, and trade shows.

— E-commerce IPR enrolment

    E-commerce platforms are increasingly offering IP rights holders the ability to enrol their brands into a platform's internal brand protection mechanism. These tools typically offer a brand owner the ability to a) prevent sellers from listing products featuring a brand name without proof of authorization from the rights holder (e.g. a licence or invoice), b) removal of infringements automatically in the background and expedited notice and takedown measures when filed by the brand owner.

— Market inspection

Inspections in local markets, including legitimate sales channels from time to time or on a regular basis.

— Due diligence

Take comprehensive steps to investigate new business partners to eliminate possibilities of manufacturing or selling unauthorized product, counterfeit products.

— Supplier audit/distributor audit

Auditing suppliers and distributors is essential to uncover any misuse of the brand owner's IP rights and illegal sourcing and distribution of products in a timely manner. Regularly reviewing contracts with suppliers and distributors to ensure that they adequately address IP matters and stipulating the penalties and remediation mechanisms for breaches is also necessary.

— Investigation: online investigation/offline investigation

An investigation into suspects collects detailed information about counterfeiting activities. At the same time, it provides evidence to support possible enforcement actions as the next steps.

— Customs training

Providing training to customs officers aims to educate them about brands and products so that they have sufficient knowledge to profile the IP risks related to the brand and raise reasonable doubts about potential IP infringement.

— Customer awareness

Maintain ongoing communication with customers/clients to ensure they are informed about where to purchase authentic products, and where they should exercise greater caution.

— Codes of conduct

Encourage and support the implementation of codes of conduct by online sellers and communicate the best practice to all parties.

8.2 Enforcement actions

Enforcement actions can be conducted online, offline or both, depending on the business needs and resources, and judicial limitations. It is possible for counterfeit sellers to have both an online and offline presence. Therefore, it is recommended that brand owners consider implementing a mixture of online and offline enforcement actions, depending on the expected outcome and previously mentioned limitations.

Online enforcement actions, which are offered by many online-monitoring service providers, can include takedown procedures and delistings of online listings and websites, and possibly dispute resolutions. Typical offline enforcement actions are on-the-ground investigations, market sweeps, raids, goods seizures, and litigation activities. Law firms, customs and law enforcement can assist when considering taking such actions.

Apart from working with legal entities, brand owners can also take independent actions like collaborating and sharing intelligence with various governments and quasi-government organizations, and becoming a member of anti-counterfeiting groups.