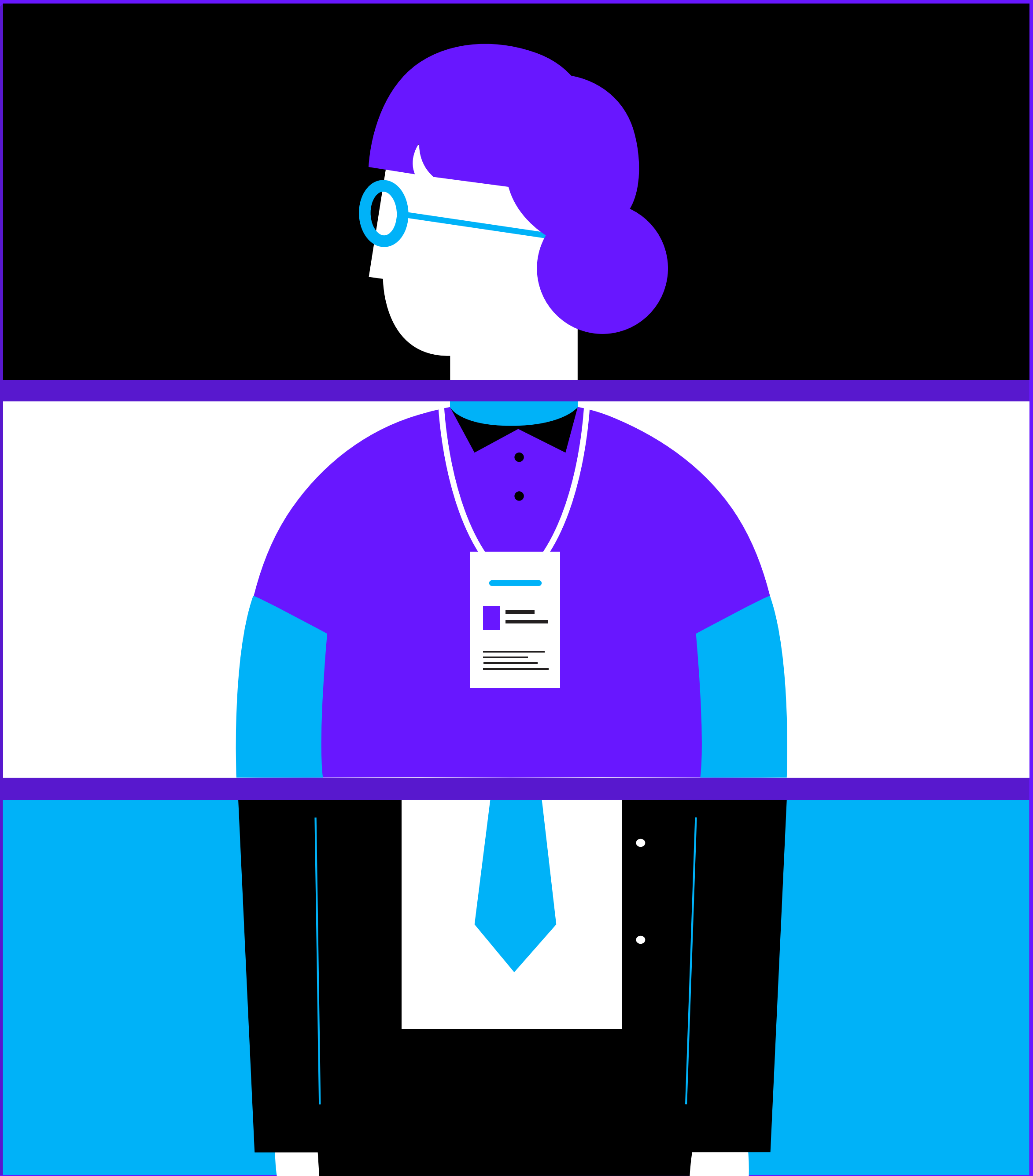
MarkMonitor
*Protecting brands in the digital world*

Clarivate Analytics

MarkMonitor Online Barometer

# The future of online brand protection

## Threats, trends and business impact



## Contents

## An evolution in online protection is under way.

## Driven by advances in the internet and the proliferation of social media, a barrage of dangers — from phishing, fraud and piracy to counterfeiting and impersonation — are impacting consumer trust, market reputation and bottom line.

Having a plan in place is more important than ever given a rapidly changing threat landscape and the next generation of online criminals constantly seeking new ways to take advantage of brands (and customers) to beat any protection mechanisms companies have in place.

## The importance of online brand protection

The focus of protection plans has changed for many brands with consumer-centric approaches. We wanted to understand how decision makers view brand protection, find out what changes they see and to discover what the future might look like.

With this in mind, we commissioned independent research firm, Vitreous World, to survey 600 marketing decision makers representing cross section of industries, across the U.K., U.S., Germany, France and Italy.

**Figure 1: Businesses that have an online brand protection strategy in place**

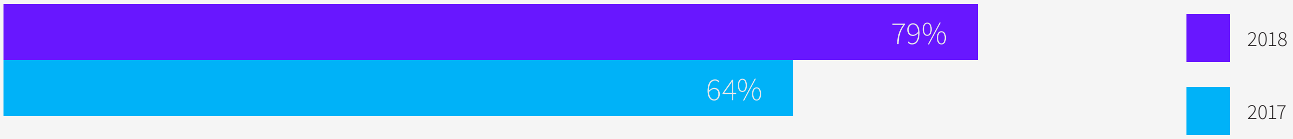
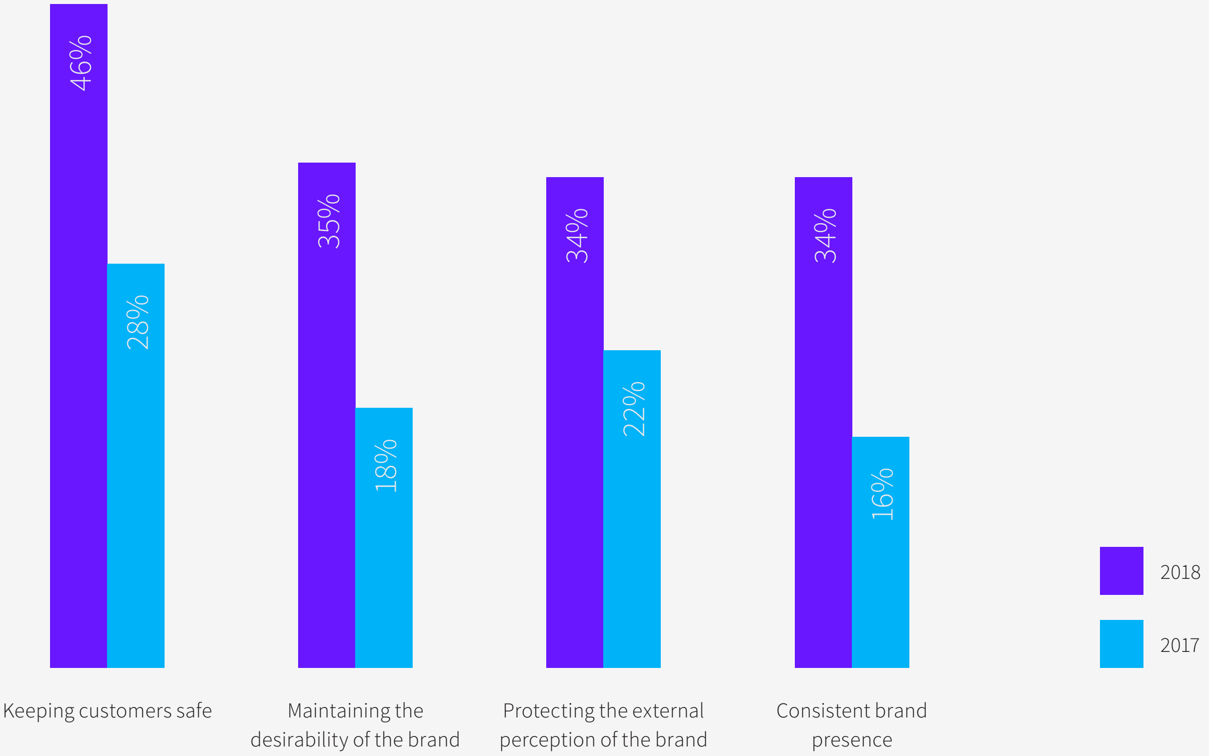


**Figure 2: Primary business objectives**



## Departments involved in brand protection

For brands, protecting their name and their consumers remains paramount. However, today, online protection is more often addressed from within multiple departments of an organisation. What's more, implementing a protection strategy requires buy-in and support from top management along with involvement from multiple areas of the business.

Today, that support has become more warranted than ever; opting to implement a brand protection strategy is now a board-level concern, due to the sheer number of angles from which attacks stem.

| | |
|---|---|
| IT Security / Trust / Risk | 55% |
| Marketing | 44% |
| Brand communications | 38% |
| Legal | 37% |
| Board | 30% |
| Unified approach | 22% |

## Snapshot of key findings

**The role of brand protection is expanding, and boundaries between departments are blurring**

72%

Said that brand protection has gained attention following a general increase in cybersecurity focus

90%

Think that the responsibility for brand protection will change over the next year

46%

Said there would be more involvement from the board

46%

Said there would be more involvement from IT and security teams

82%

Said brand protection would change to include new threats around security and fraud in the next year

## Snapshot of key findings

### Brand protection is becoming more consumer-focused

Most important consideration is keeping consumers safe

46%

Shopper behaviour plays a major role in prioritising brand protection programmes

84%

### Brands are future-focused

64% of respondents believe that infringement has increased over the last year. In addition, brands are incorporating new technologies in their online brand protection strategies including:

Artificial Intelligence (AI)

39%

Big data

37%

Machine learning

33%

Dark web monitoring

25%

## The future of brand protection

As threats expand, brands shift focus to incorporate new technology. There is also evidence of more involvement from additional stakeholders within the business. Research indicated that 72% of marketing decision makers believe that brand protection has gained attention following a general increase in cybersecurity focus.

These threats affect all businesses, regardless of size or industry. Importantly, this threat to businesses is increasing at a rapid rate, with research suggesting cyberattacks doubled in 2017[1].

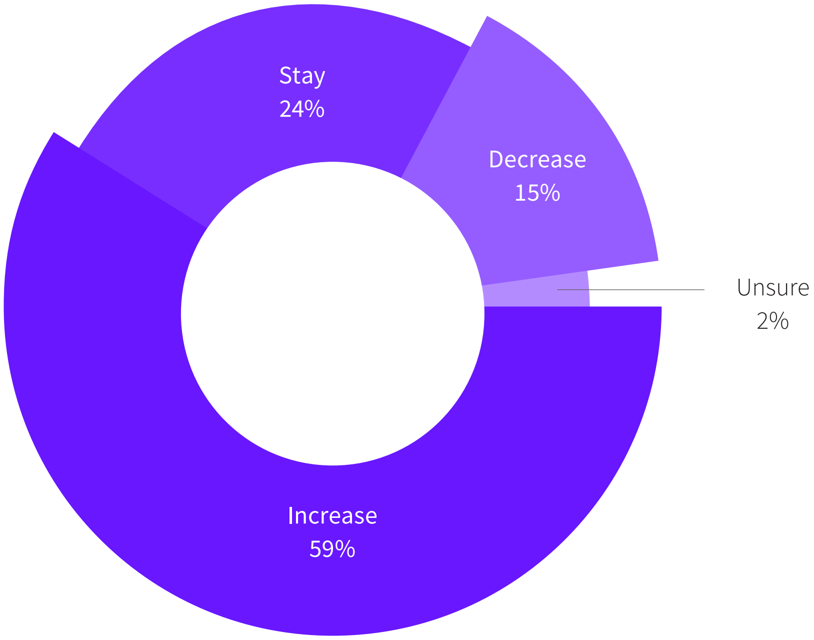
In fact, the World Economic Forum named cyberattacks as one of the top five risks to global stability[2]. As a result, the impact on brand protection could be significant and shows that it needs to be integrated with wider cyber security strategies to ensure both are aligned to the benefit of the business and plug any gaps that may occur.

A high proportion of respondents also said that brand protection itself would change in the future. Ninety-nine percent of brands believe the responsibility for brand protection will change over the next year, with 46% saying there would be more involvement from the board and IT security teams.

This is particularly relevant considering marketing decision makers think the bulk of future brand protection threats will come from social media, phishing, unauthorised websites, online marketplaces and apps (see figure 5).

> *58% believe the importance of having a brand protection strategy will increase in the next five years.*

**Figure 3: Perception of change in the importance of having a brand protection strategy in the next five years**



[1] https://www.infosecurity-magazine.com/news/cyberattacks-doubled-in-2017/
[2] http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

### The era of consumer centricity

The primary objective of a brand protection strategy, according to research, is to keep consumers safe. This year 46% of respondents cited this as the main reason, up from just 28% from similar research carried out last year. This speaks to the relevance of new, consumer-focused approaches which target criminal activity where the consumer is most exposed to threats. To 84%, consumer behaviour plays a major role in how their brand protection programme is prioritised.

Applying this same approach to dealing with infringements has the potential to make brand protection more effective. By prioritising infringements based on this consumer-centric view — that is focusing on infringements where consumers are most likely to encounter them — brands can be more effective and save time and resources because they are not trying to remove every single infringement. It also helps better protect the consumer.

> *To 84%, consumer behaviour plays a major role in how their brand protection programme is prioritised.*

In spite of a new focus on consumer-centric brand protection, many businesses still report a focus on overall enforcement totals that include pages and listings less relevant to users. Thirty-four percent say they prioritise detections and takedowns based on the most visible sites and listings from a consumer perspective.

### The role of technology

From brand protection specialists who develop solutions to businesses tackling the challenge in-house or with a third-party, success can come down to the right technology. As the threat landscape changes, and counterfeiters, pirates and cybercriminals become more sophisticated, brands can't afford to be left behind and suffer the ill-effects of not keeping current with the shifts in risk and threats. This attitude is reflected in the results of a future-focused question around budget allocation for brand protection.

Almost a quarter of respondents said they would spend most of their budget on new technology, and 85% of brands have incorporated new technologies into protection efforts, including artificial intelligence (39%), big data (37%), machine learning (33%), and dark web (29%).

The likes of AI, machine learning and big data analytics can be used to monitor the threat landscape in a more efficient and effective way, giving brands a more proactive approach for dealing with threats, especially concerning phishing. When it comes to the dark web, while the landscape may not be new, it is new when it comes to monitoring for threats. The dark web is not just an illicit market place for physical goods and services, but also confidential data and intellectual property, that can seriously damage a brand. Proactively monitoring this area of the web ensures brands are better able to mitigate risk and can quickly neutralise any threats.

## The bigger brand protection picture

In today's omni-channel environment, where brands have a presence across different channels, the scope of protection is even greater. The bigger the presence across channels, the bigger the threat — in fact, almost two-thirds of respondents said they believed infringement had increased in the last 12 months. This attitude was more prominent amongst U.S. (75%) and French (71%) respondents.

> *64% of brands say infringement has increased in the last year.*

To understand more about the scale of the threat, we asked respondents which of the channels used for brand communications had been subjected to infringement and abuse over the last 12 months.

Websites experienced the highest levels of infringements (45%), followed by email (42%), social media channels (34%), mobile apps (31%) and online marketplaces (27%). In fact, 55% of respondents said they were paying more attention to their domain name strategy and were managing it more actively in light of the prevailing cyber threat. A further 14% said they were working on changing their approach. Domain management needs to form a key part of an overall brand protection strategy; not just for security reasons, but also in terms of maximising portfolio values and keeping costs down. As a result, it's important to select the best approach, depending on the needs of the brand and whether being proactive or defensive has more value. What this also demonstrates is that threats have broadened and the lines between brand protection and cybercrime are becoming blurred pointing to an approach that incorporates both elements.

When it comes to cybercrime, the majority of businesses (86%) have experienced phishing attacks in the last 12 months. This included brand impersonation websites, malware distribution, business email compromise scams, SMS text (smishing) and phone impersonation (vishing).

Increasingly, brands think activity on the dark web poses a threat to business. More than half of respondents (56%) said this, while a further 61% said they were actively monitoring dark web intelligence for threats and brand-related activity.

This was more prevalent amongst French (74%), Italian (72%) and U.S. (70%) respondents. This is a rather important step forward for brand protection; one of the main challenges when it comes to the dark web is that there is no enforcement mechanism in place for brands to protect themselves effectively. However, by actively monitoring and using the right technologies based on AI and machine learning, companies can mitigate the risk that the dark web poses by identifying threats early and dealing with them quickly and effectively — whether that's identifying stolen customer details, intellectual property or plans for a cyber attack.

86%

Have experienced phishing attacks in the last 12 months

56%

Think activity on the dark web poses a threat to business

61%

Actively monitoring dark web intelligence for threats and brand related activity

## Snapshot of the impact

### Channels affected by brand infringement

In the last year, brands reported negative effects of infringement across multiple channels, signaling an increasing scope of threats.

Websites
45%

Email
42%

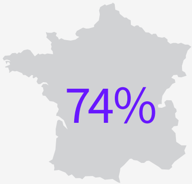
Social media channels
34%

Mobile apps
31%

Online marketplace
27%

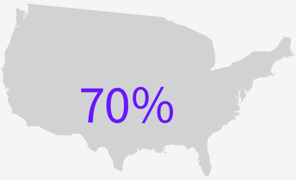
### Countries actively monitoring dark web

By country, it is clear that brands are taking a more proactive approach to consumer safety online. These countries reported having actively monitored for dark web or brand related threats.



France

Italy



U.S.

## A look back: Benchmarking 2017 results

In 2017, similar research gauged the opinions of more than 900 marketing decision makers in nine countries.

Research painted a picture of an ever-evolving landscape where the importance of online brand protection is only growing. While this is reflected in this current study, we also found in 2017 that brand protection was undervalued within the organisation and that keeping a brand safe will become increasingly difficult over the next five years.

There were definite commonalities in both sets of research, particularly around increased threat levels, enforcement and cost of infringement.

Consequences of combined threats to brands and cybercrime includes loss of customer trust and damage to market reputation, which are both difficult to quantify. However, impact on bottom line causes a tangible effect on the business.

The proportion of lost sales revenue best describes the severity of the threat. Looking specifically at phishing attacks, 38% of the 2018 respondents said they had lost up to 10% of revenue as a result; 22% said they lost up to 25% and 14% said they lost up to 50% of their revenue.

A key component in beating phishing is employee education; after all, phishing only works if someone clicks on the offered link or downloads the attachment. Incorporating cybersecurity best practices into a brand protection plan can therefore go a long way towards making defence strategies more effective.

It's not just phishing that is costing brands money. Table 1 details threats and includes loss of revenue figures. Looking at the first four elements, there are some significant differences between figures from 2017 and 2018, signalling the growing threat and a need for comprehensive protection.

That said, brands are not complacent. Last year, 64% said they had a protection policy in place. This year, that figure rose to 79%. Looking at company size, those brands employing up to 250 staff were nearly just as likely (77%) to have a plan in place as enterprises (83%).

**Table 1: Quantifying the threat in 2018**

| | Lost sales to counterfeit or pirated goods | Lost traffic to cyber squatted sites | Increased cost of paid search advertising due to ad fraud | Counterfeit sponsored adverts appearing on social media platforms | Lost sales dues to digital piracy |
|---|---|---|---|---|---|
| Experienced | 15% | 15% | 19% | 20% | 17% |
| Loss up to 10% of sales revenue | 32%<br>*(32%)** | 29%<br>*(32%)** | 34%<br>*(33%)** | 30%<br>*(33%)** | 42% |
| Loss up to 25% of sales revenue | 23%<br>*(39%)** | 26%<br>*(36%)** | 31%<br>*(33%)** | 32%<br>*(31%)** | 20% |
| Loss up to 50% of sales revenue | 32%<br>*(17%)** | 22%<br>*(16%)** | 18%<br>*(16%)** | 18%<br>*(16%)** | 21% |

** 2017 figures*

## The rise of enforcement actions

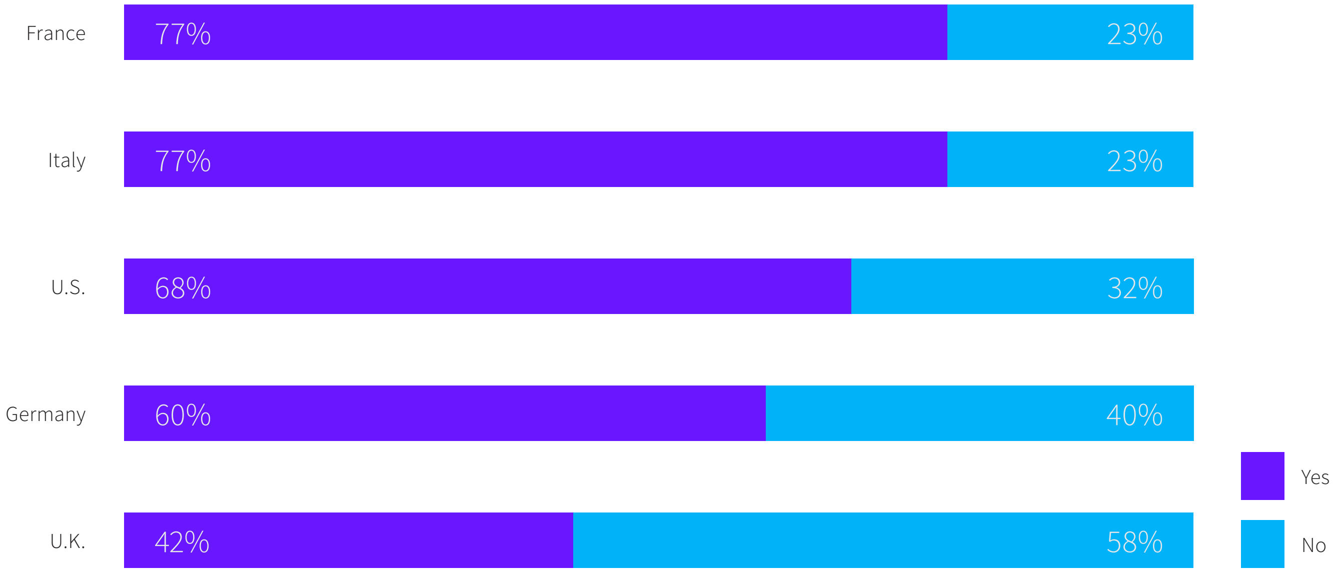
In 2018, 61% of brands said they had taken action against counterfeiters over the last year. An increase of 9% over the 2017 figure, this may signal an imminent implementation of better strategies, expanding threats or a combination of both.

When asked about the success of these efforts in 2018, reactions were mixed; a total of 2,660 cases were successful (74% said one or more cases was successful) due to infringing content being taken down — with takedowns in Germany (11.9) and the U.S. (10.0) occurring more frequently. A further 1,995 were not successful (60% of this number said one or more cases was unsuccessful), while 2,470 cases resulted in financial compensation.

## Where are the threats coming from?

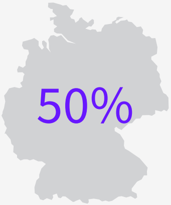
In a multi-channel world, the threats are many. We asked respondents where the majority of today's threats were targeted. The top three threats were identified as phishing (37%), social media (36%) and unauthorised websites (34%). Looking at the differences between countries, phishing was more prevalent in Germany (50%) and Italy (43%), while social media threats are more prominent in Germany (47%) and the U.S. (43%), and the U.K. (36%) and France (41%) are more likely to be affected by threats from unauthorised websites.

**Figure 4: "Has your organisation taken legal action against counterfeiters in the last 12 months?"**

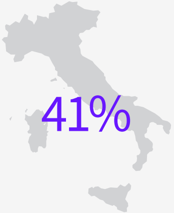


## Main threats to brand protection in the most targeted countries

Phishing
37%

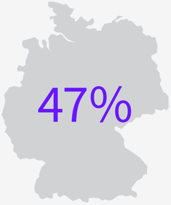


Germany

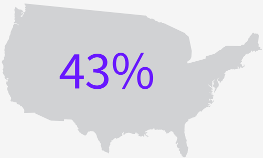


Italy

Social media
36%

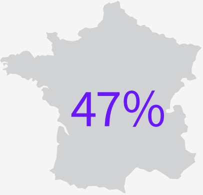


Germany

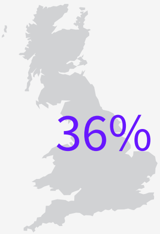


U.S.

Unauthorised websites
34%



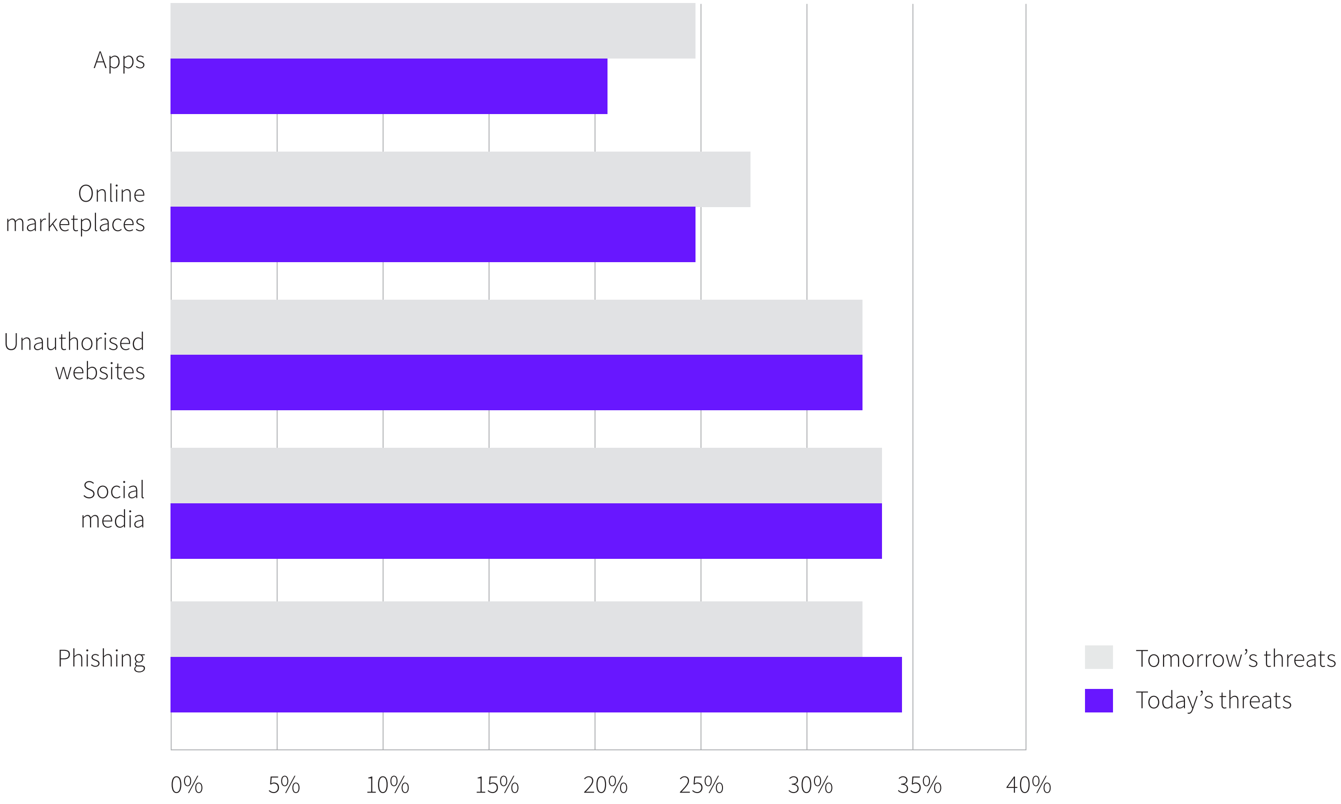
France



U.K.

When asked about future threats, the responses were not vastly different to what brands were currently dealing with. However, threats from social media were identified as the main concern, with phishing being pushed to second place.

**Figure 5: Today's and tomorrow's threats**



The threat posed by phishing is something that brands are also addressing when it comes to allocated budget. In the next five years, brands are more likely to spend money on hiring people with the right skills to help brand protection efforts (28%), protecting domain names (26%) and fighting phishing (25%). Six percent still do not have a budget.

In terms of budget allocation for the next five years, nearly a quarter of those surveyed are looking to new technologies to help them protect their brand.

## Conclusion

The consequences of getting a brand protection strategy wrong can be dire: loss of trust, damage to reputation and, of course, negative impact on revenue. Whether you are working with in-house experts and departments, with an external brand protection specialist, or both, ensuring your business and customers are safe is becoming more difficult as the threats (and their sophistication) increase. This means earning buy-in and involvement from the entire business.

The real challenge is to educate decision makers that sheer volume of infringements isn't necessarily what counts for a business' bottom line. Not only do brands typically not have the resources to address all infringements, doing so is nowhere near as impactful as removing infringements from the places where users are more likely to see them. Key questions to consider in developing this type of approach include: are you targeting the same listings your customers see (the first page of search results), can you see what your global customers see, can you easily identify infringements, and can you identify high value targets?

## Methodology

600 marketing decision makers were surveyed in September/October 2018 for opinions and attitudes towards brand protection — both as it stands now and what lies ahead.

Research was conducted by independent survey firm, Vitreous World, and data was collected via online interviews. Respondents were taken from a cross section of industries and countries, including the U.K., U.S., Germany, France and Italy.

## About Clarivate Analytics

*Clarivate Analytics* is the global leader in providing trusted insights and analytics to accelerate the pace of innovation. Building on a heritage going back more than a century and a half, we have built some of the most trusted brands across the innovation lifecycle, including *Web of Science, Cortellis, Derwent, CompuMark, MarkMonitor* and *Techstreet*. Today, *Clarivate Analytics* is a new and independent company on a bold entrepreneurial mission to help our clients radically reduce the time from new ideas to life-changing innovations.

## About MarkMonitor

*MarkMonitor,* the leading enterprise brand protection solution and a *Clarivate Analytics* flagship brand, provides advanced technology and expertise that protect the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the Web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose *MarkMonitor* for its unique combination of advanced technology, comprehensive protection and extensive industry relationships to address their brand infringement risks and preserve their marketing investments, revenues and customer trust.

To learn more about MarkMonitor, our solutions and services, please visit **markmonitor.com** or call us at **1-800-745-9229**

**North America**

| | |
|---|---|
| Philadelphia: | +1 800 336 4474<br>+1 215 386 0100 |

**Latin America**

| | |
|---|---|
| Brazil: | +55 11 8370 9845 |
| Other countries: | +1 215 823 5674 |

**Europe, Middle East and Africa**

| | |
|---|---|
| London: | +44 20 7433 4000 |

**Asia Pacific**

| | |
|---|---|
| Singapore : | +65 6775 5088 |
| Tokyo: | +81 3 4589 3100 |

11.2018

**clarivate.com**

**MarkMonitor**
*Protecting brands in the digital world*

Clarivate
Analytics