MarkMonitor™

| A Clarivate Analytics company

2019 | Global Business Survey

The online brand protection life cycle
Domain and cybersecurity edition

Contents

This report examines the domain landscape, challenges brands face when securing and managing domains, the impact of legislative changes and related lifecycle elements – infringement, fraud and brand abuse.

Introduction

The domain space has continued to evolve since its beginnings 1985, when the first domain name was created.[1]

Today, businesses are getting more innovative with catchy .Brand extensions, such as .monster [2]. The launch of generic top level domains (gTLDs) in 2013, along with ongoing legislative and political changes and cyber threats, has also unveiled a new era of online protection challenges.

For brands, this means more time and resources are being spent on managing and securing domains. A core to brand identity, they must be protected at all costs and form the cornerstone to any broader business strategy.

What are the best ways to approach domain portfolio management and broader online brand protection efforts? How do different brand protection lifecycle elements, from navigating infringement, fraud and wider brand abuse, influence each other?

The answer lies in aligning these elements into a holistic view of the organisation and includes everything from domain registration, the securing of those names, monitoring them for abuse and mitigating risks to users and intellectual property.

To find out how businesses tackle these challenges today, we commissioned independent research firm Vitreous World to survey 700 IT, legal and marketing decision makers from a cross section of industries across the U.K., U.S., France, Germany and Italy.

This report examines the domain landscape, challenges brands face when securing and managing domains, the impact of legislative changes and related lifecycle elements – infringement, fraud and brand abuse.

[1] https://www.edn.com/electronics-blogs/edn-moments/4410016/1st--com-domain-name-is-registered--March-15--1985

[2] https://domainnamewire.com/2019/04/01/yes-domain-names-really-can-end-in-monster-now/

Snapshot of key findings

Online security is an increasing issue for brands, especially around domains

62%

of brands have seen impacts of cybercrime in the last 12 months

23%

of organisations have experienced a cyber attack targeted at their domain

48%

believe brand infringement has increased over the last 12 months

46%

said the cyber threat has influenced their domain strategy

IT, legal and marketing decision makers recognise the importance of domain management and security but noted measurable challenges

- 43% of respondents said their domain portfolio was vital to brand building and maintaining customer trust
- Security (56%), cost (40%) and keeping track of domains (34%) are the most cited challenges when it comes to domain management
- 56% of brands own up to 100 domains, yet only 18% say more than three-quarters of their domains are active
- 32% of organisations don't monitor domain value as part of domain management

Domain management and security are largely siloed

- Responsibility for domain management largely falls to IT / IT security (46%), followed by legal (16%), a combined effort (13%) and marketing (13%)
- The renewal process is also an issue: 26% of respondents rely on renewal notices, 21% rely on one person to do this, and just 25% have a plan in place that involves collaboration between departments
- 25% cite lack of budget as one of the main challenges in monitoring an effective brand protection programme

The landscape is changing, becoming bigger and more complex

39%

have registered a gTLD and, of that number, 32% have experienced brand impersonation and abuse against it

39%

of brands say Brexit has impacted their domain strategy

46%

of brands say GDPR has impacted their domain strategy, with 18% of that number finding it harder to enforce against infringements

Setting the scene

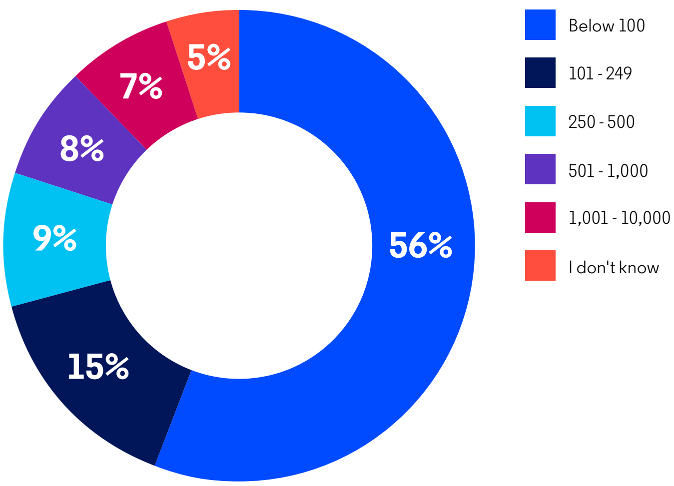
Why are domains so important to modern businesses?

At a base level, domains provide organisations with a unique description that clearly distinguishes them from competitors. However, larger brands, especially those that operate globally, find the domain management process more complex than simply choosing and registering an initial domain.

Sub-domains, name variations, domains for campaigns, defensive registrations and regional domains all need to be considered, registered and managed. The result is that organisations deal with large domain portfolios that are cost and time intensive in terms of management and renewals.

This is reflected in the number of domains brands currently own. The majority (56%) of respondents in the research said they owned fewer than 100 domains, while a further 15% own 100-249; 9% own 250-500; and 8% between 500-1,000.

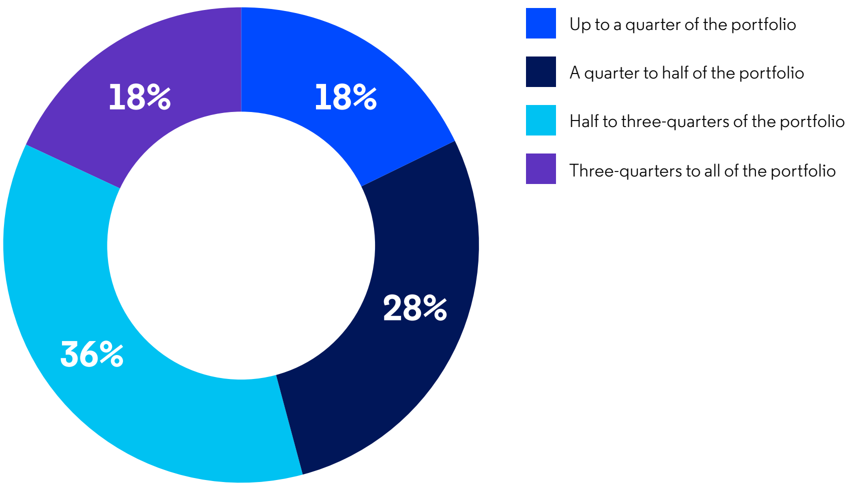
How many domains does your organisation own?



Despite the number of domains, not all of them are currently active. Almost one-fifth (18%) of respondents said up to 25% of their portfolio was active, while a further 18% said between 76-100% were active. The bulk of respondents fell in between, with 28% stating that 26-50% of their portfolio was active, and 36% stated 51-75% was active.

Managing domains and the role they play in building awareness and maintaining customer trust is essential. It is, however, a costly endeavour. If brands have domains that aren't adding any value to the organisation yet are still being paid for, is that resource better spent in securing and managing the core domains?

How much of your domain portfolio is currently active?



This sentiment is reflected in the fact that brands recognise the importance of these domains; when asked what motivates their domain registration strategy, 60% said to promote new products or services; 38% said changes in the market, such as gTLD launches; 34% said reaching an international audience was a driver; and 27% said mitigating brand abuse.

The organisational view of domains was further explored by asking how their company viewed their domain portfolio. Forty-three per cent of respondents said it was a vital part of brand building and maintaining customer trust. However, almost one-quarter (23%) said it represented a security risk to the brand, 17% viewed it as a necessary evil, and 16% said it was a valuable IP asset. All responses highlight the importance of balancing management and security.

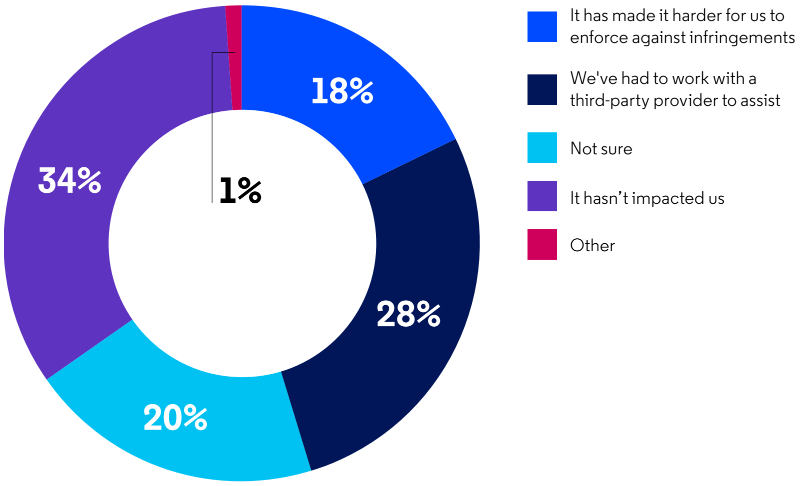
Aside from internal motivations driving domain management, there are also various external factors that shape the management process. Most notably the issues of Brexit and the General Data Protection Regulation (GDPR).

Interestingly, 61% of respondents said Brexit had no impact on their domain strategy, while 25% said they were re-evaluating their .EU strategy. This lack of impact is perhaps surprising given that U.K. organisations have been made aware by EURid, the registry manager of the .eu TLD, that they are no longer able to register new or renew existing EU domains[3].

Along the same lines, 34% of brands said GDPR hadn't affected their domain strategy, while 28% said they were working with third party suppliers for assistance. Twenty per cent weren't sure about the impact, and 18% said they were finding it more difficult to enforce against infringements.

[3] https://eurid.eu/en/news/ec-releases-communication-concerning-brexit-and-the-eu-tld/

How has GDPR impacted your domain strategy?



Which factors go into selecting a domain provider/registrar?

Service 46%

Price 45%

Cost management 40%

Optimising the domain portfolio 21%

A broader market

Organisations also need to navigate the changes to the industry itself, particularly the introduction of gTLDs and what these mean for their brands in terms of new registrations, security and management. Since the gTLD programme was launched just a few years ago, hundreds of global brands have registered new gTLD domains.

The aim of gTLDs was to help organisations differentiate themselves online by enhancing brand recognition, increasing customer trust and giving brands a better level of control over their online presence. How are they faring?

Almost four in 10 organisations (39%) have registered a gTLD, with the most prevalent challenge being measuring its return on investment cited by 34% of respondents. Other challenges here include:

- Brand impersonation / abuse – 32%
- How to mitigate the risk of abuse against the new gTLDs – 23%
- Mistrust of websites – 20%
- Lack of understanding around the gTLD landscape – 13%

In essence, gTLDs have opened up an additional avenue that brands need to consider as part of not only their domain strategy, but their online brand protection programmes as well.

The complexity of domain management

The challenges around domain management don't stop there. Managing domains also calls for registration, monitoring and renewing. Unsurprisingly, 56% of respondents stated security was one of the main issues, followed by cost of management (40%), and management itself (34%).

Demonstrating returns on investment

In a world where ROI is crucial, organisations strive to ensure they are optimising and streamlining the domain management process.

Given that this is such a critical part of operations, how is the management and renewal process approached? And is it the most effective method for the brand?

Name your challenges when it comes to domain management

Security 56%

Knowing which domains to register 22%

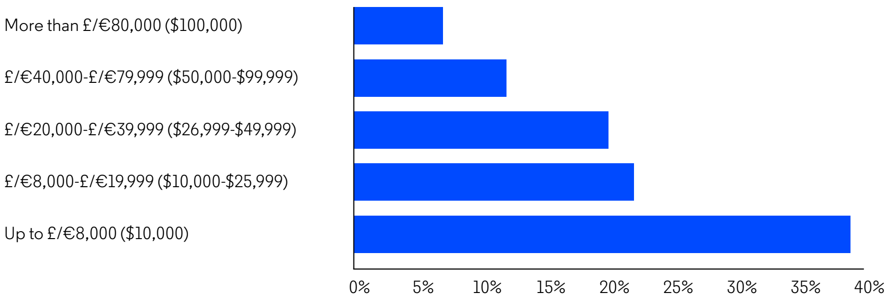
Cost management 40%

Optimising the domain portfolio 21%

Keeping track of domains (management) 34%

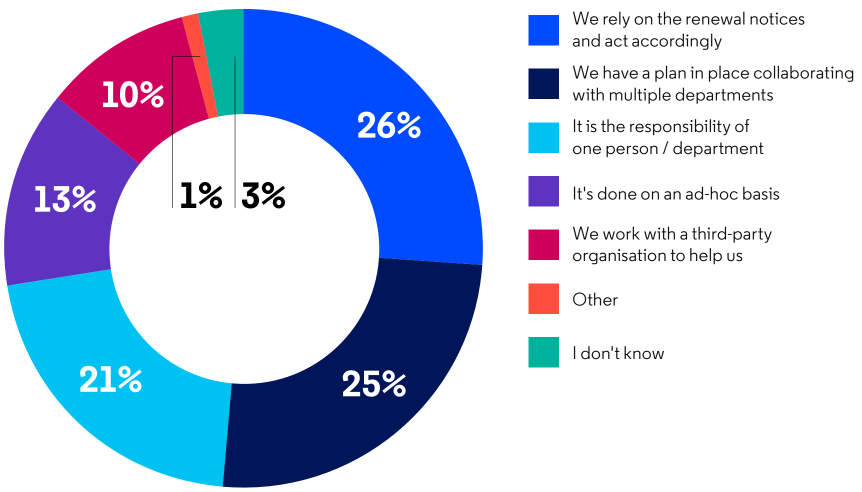
Understanding the new gTLDs 19%

Money spent per year on domain management



More than one-quarter (26%) of respondents rely solely on renewal notices, while a further 25% subscribe to the industry best-practice approach and have a plan in place and collaborate with multiple departments. Twenty-one per cent of brands give the responsibility of management and renewal to one person; 13% approach it on an ad-hoc basis; and 10% work with a third-party provider to help them.

How does your organisation approach domain management and renewal?



Delegating this crucial task to just one person has a number of drawbacks; without a holistic approach it is difficult for this individual to see which domains are more important than others, which are being used and which domains can be sold off. It also means that if this staff member leaves the organisation or moves roles the knowledge around renewals and management could be lost; important notices could get lost in a defunct email box; and the organisation could miss renewal deadlines and face potentially devasting consequences.

When it comes to board involvement around domain management and security, the importance is clear; 43% said it was an important board-level issue with hands-on involvement from directors. A further 35% said it was understood by the board but that they were not involved, 19% said it wasn't a board-level issue in their organisation, while just 4% said the board didn't understand the importance.

Getting board buy-in and support is crucial for securing budget for management and security, as well as for ensuring that the domain process is included in the overall brand protection strategy of the business. This is particularly important when it comes to optimising the portfolio, getting the most value out of it, and having the resources to dedicate to this task.

One such way is monitoring the value of domains. This approach helps brands streamline their domain portfolios and identify domains that are no longer adding value to the organisation.

Sixty-two per cent of brands said they did monitor the value of their domains. Of that number, 28% said they did it to identify and retire low value domains, while 22% said they monitored value to ensure their core brands were protected. While this is encouraging, 32% (possibly more as 6% of respondents didn't know if they monitored value) are potentially missing out on opportunities around streamlining and optimising their domain portfolio, in terms of offloading old names and ensuring core names are better protected.

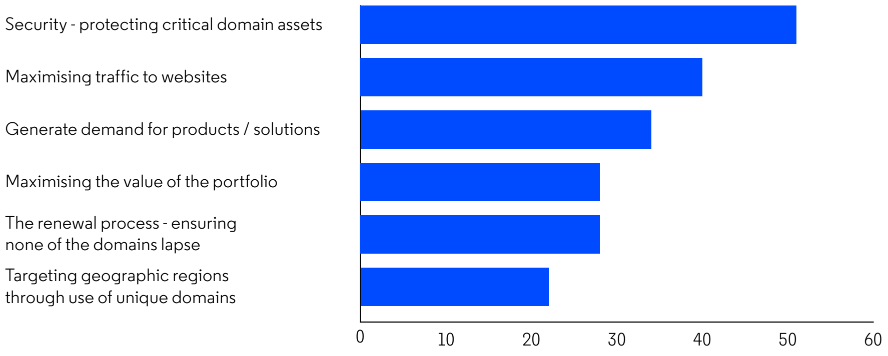
Secure the domain, secure the brand

The domain management process needs to form part of a wider brand protection programme, especially with the increasing importance of cyber security. It also means there are several elements that need to be considered throughout the management of the domain portfolio – the most important of which is security.

Respondents agreed. More than half (51%) said that protecting critical domain assets was the most important issue in domain management.

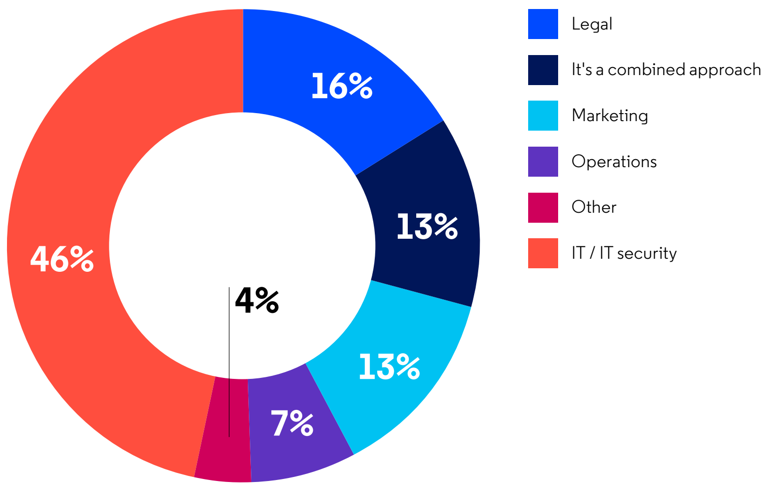
Forty per cent identified maximising traffic to websites as the key area; 34% identified generating demand for their products or solutions; 28% identified maximising the value of their portfolio; and another 28% named the renewal process as key.

What are the most important aspects of domain management?



The focus on security is also reflected in which areas of the business are responsible for managing domains. Overwhelmingly this task falls to IT / IT security (46%), followed by legal (16%), a combined effort (13%) and marketing (13%).

Who within the organisation is mainly responsible for managing domains?



Hackers look to the DNS

Increasingly, the Domain Name System (DNS) is becoming a target for hackers and cyber criminals, and with the increasing cyber threat, brands need to balance traditional domain management with online security as well.

The threat is real. The Internet Corporation for Assigned Names and Numbers (ICANN) issued a warning earlier this year, calling out "an ongoing and significant risk to key parts of the Domain Name System (DNS) infrastructure"[4].

Threats include registry breaches, domain hijacking, phishing attacks, and use of malware to collect credentials, all of which highlight the need for having the right security measures in place and working with a corporate registrar who also has the expertise and technologies in place to protect its customers.

This is reflected in the figures; almost one-quarter (23%) of respondents indicated their organisation had suffered an attack targeted at their domain. The consequences of these attacks varied from loss of data (48%) and damage to customer trust (38%), to loss of revenue (37%) and damage to reputation (32%).

There is awareness of the cyber threat and its impact on domains. Only 14% of respondents didn't know what security measures were in place to protect their domains, while the remaining sample indicated their organisation used a variety of measures, including:

41%
Two-factor authentication

35%
Name server monitoring

31%
Single-sign on

28%
Registry locking

4 https://www.icann.org/news/announcement-2019-02-22-en

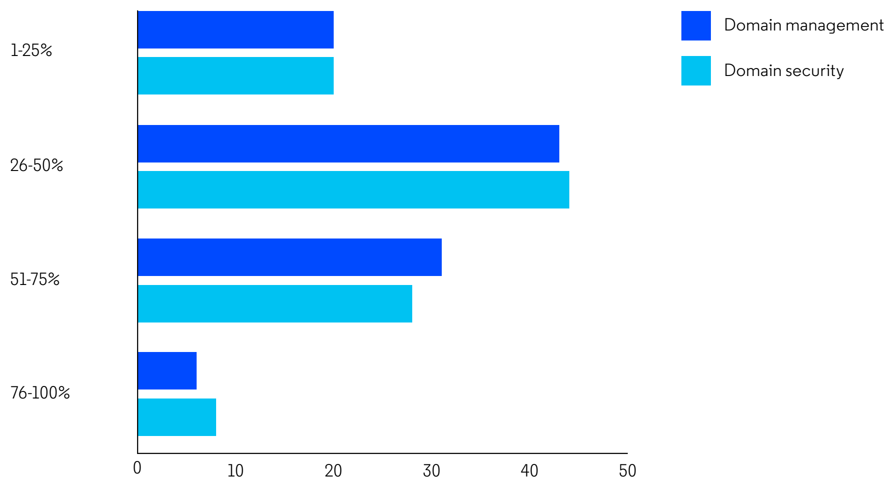
The bigger brand protection picture

The cyber threat doesn't just affect domains, but all aspects of the organisation as well. As a result, online brand protection is evolving to accommodate these changes and help mitigate the risk.

However, only 44% of respondents indicated they had budget dedicated to online brand protection. Delving deeper, 43% of the sub sample said they dedicated 26%-50% of their total online brand protection budget to domain management, while 44% said they dedicated the same proportion to domain security.

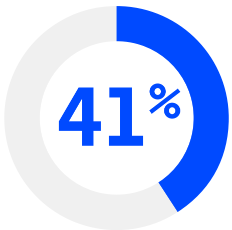
A further 49% said they didn't have a dedicated online brand protection budget, which potentially leads to gaps in safeguarding the brand and not being able to manage abuse, fraud and cyber threats. While they may be able to react to issues and allocate budget on an ad hoc basis, brands need a more proactive approach to brand protection to ensure they are able to effectively mitigate the risk.

How is your domain protection budget allocated?

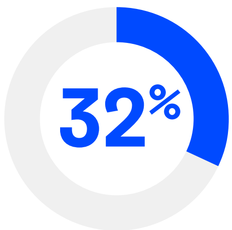


Lack of budget was cited by 25% as a challenge in monitoring an effective brand protection programme. Other issues include: lack of resources (27%), lack of knowledgeable staff (26%), and difficulty in quantifying infringements (24%).

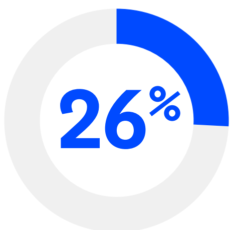
Given the severity of the threat, we asked decision makers how they approached brand, domain and fraud protection online. They said:



approach it holistically



address the elements in isolation



align it to their cyber security plans

While brands are placing large emphasis on the cyber security aspect of online brand protection, the same focus needs to be given to their domain portfolio.

The latter figure is put into clear focus looking at the fact 46% of respondents in the research say the cyber threat has influenced their domain strategy. Of that figure, 34% said they are managing their domain strategy more accurately and 12% said they are changing their approach. In fact, 42% of respondents said the increased attention on cyber security meant brand protection was getting more attention in their organisation.

While domain security issues were certainly a concern, respondents cited a number of other issues. Fraud, in the form of malware and phishing, was cited by 61% as one of the main threats to their organisation. This was followed by piracy (37%), domain impersonation (32%), brand abuse (27%) and the dark web (18%).

These threats were seen to come predominantly from Asia (58%), of which 35% were from China, Europe (24%), the US (20%), Africa (17%) and the Middle East (16%). This is important to keep in mind considering new domain name registration rules implemented in China in 2017[5]. While these changes could reduce the risk of fraud, it doesn't eliminate unauthorised uses of their brands online in the country.

5 https://www.webmasterworld.com/asia_pacific_search_engines/4874829.htm

In terms of frequency, 6 in 10 brands have felt the impact of some kind of cybercrime in the last 12 months. This includes phishing (28%), false association (13%), brand/logo confusion (13%), keyword hijacking (13%), traffic diversion 12%, and lost traffic to cyber squatted sites (10%). Nearly half (48%) of decision makers in the survey believe that brand infringement has actually increased over the last 12 months.

Looking ahead, respondents believe they will spend most of their brand protection budget on four key areas over the next five years.

26%

Fighting phishing fraud

26%

Implementing new technology that could impact brand protection

25%

Protecting domain names and company IP

22%

Combatting piracy

Conclusion

The lifecycle of online business protection spans from the establishment of a brand and its domain registrations all the way to managing and securing a portfolio.

As part of that cycle, additional elements feed and shape the process of protection, including infringement, fraud and brand abuse. Keeping a brand healthy, safe from cyber attacks and optimised – to ensure a return on investment – is critical in meeting the expectations of customers, maintaining brand identity and reputation, and safeguarding the bottom line.

In surveying IT, legal and marketing decision makers, it is clear that domain security and management are top of mind as part of a wider brand protection programme. Related challenges can include budgeting, allocating the right resources and ensuring that the right people in the organisation are collaborating to streamline and control the process.

Against the backdrop of cyber threats and other types of brand infringement, domain management and security have never been more important. Working with the right partner proves key to optimising any domain portfolio and addressing vulnerabilities.

Next steps

This report highlights the influence of the cyber threat on domain strategy and online brand protection as a whole. But what are the key considerations for brand owners?

- Domain strategies need to form part of wider brand protection initiatives
- Domains should be managed in a collaborative effort between departments including IT, IT security, marketing and legal
- Domain portfolios must be secured and managed to ensure they continue to add value to the business
- Domain value should be monitored to ensure active, core domains are protected and managed, while other domains are offloaded to optimise the portfolio

Are you looking to evaluate your current domain portfolio? At MarkMonitor we have a team of experienced professionals who can help you assess and streamline your portfolio to get the most value from your domains. We can help you register, secure and manage your domain portfolio, and execute a wider online brand protection strategy. Get in touch with us today to find out how we can assist your organisation.

Methodology

700 IT, legal and marketing decision makers were surveyed in April 2019 to gauge attitudes and opinions around domain management, security and overall brand protection.

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.

MM190107 / 01

About MarkMonitor

MarkMonitor™, a leading enterprise brand protection solution, 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. MarkMonitor is a Clarivate Analytics™ company.

Contact our experts today:

+1 800 745 9229 (U.S.)
+44 (0) 1978 528 370 (Europe)

markmonitor.com