CSC

DOMAIN SECURITY REPORT

FORBES GLOBAL 2000 COMPANIES

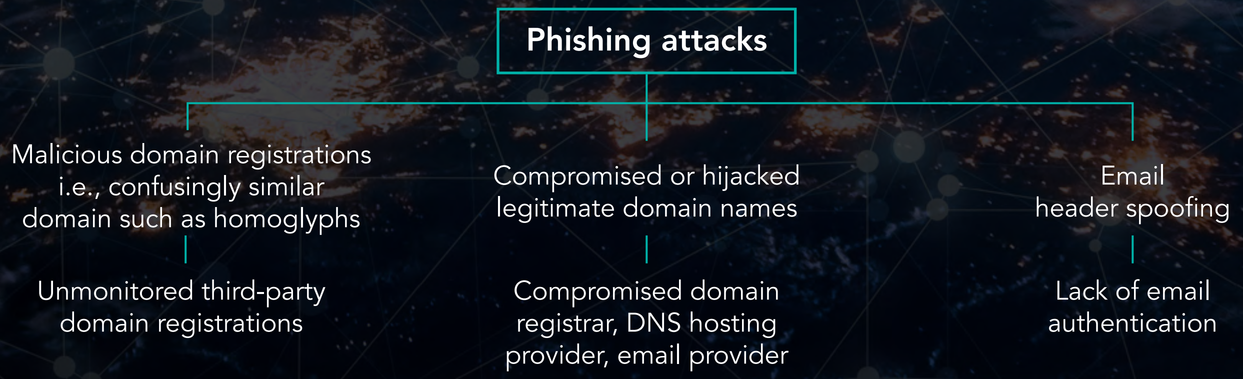
2021

Executive summary

With cyber crime on the rise, companies in 2021 have experienced increased ransomware attacks, business email compromise (BEC), phishing attacks, supply chain attacks, and online brand and trademark abuse. While domain cyber risk is rising, the level of action being taken by Forbes Global 2000 companies to improve their domain security posture has remained unchanged, leaving these companies exposed to even more risk.

Domain security is a critical component to help mitigate cyber attacks in the early stages—*your first line of defense*

According to CISA, most cyber attacks, including ransomware and BEC, begin with phishing. Although losses due to ransomware now exceed billions annually, most ransomware protection and response measures don't adequately address phishing risks in the early stages of a ransomware attack because they do not include domain security measures to protect against the most common phishing attacks. Established research shows that phishing attacks most commonly occur from a maliciously registered, confusingly similar domain name, a compromised or hijacked legitimate domain name, or via email header spoofing.



Phishing attacks

Malicious domain registrations i.e., confusingly similar domain such as homoglyphs

Unmonitored third-party domain registrations

Compromised or hijacked legitimate domain names

Compromised domain registrar, DNS hosting provider, email provider

Email header spoofing

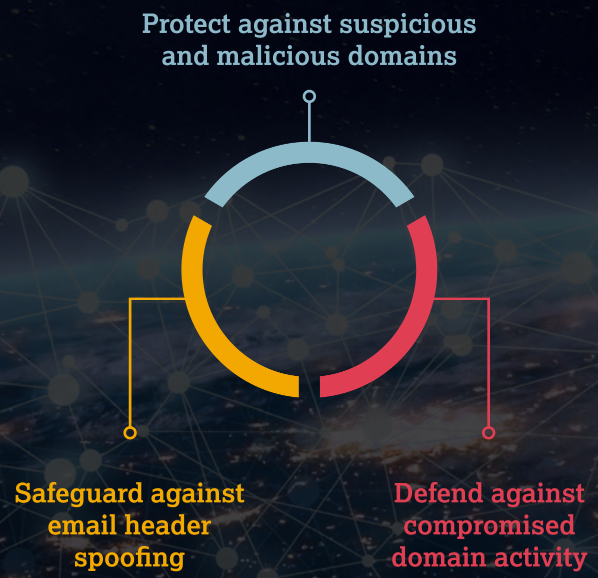
Lack of email authentication

Understanding cyber risk when it comes to your domains

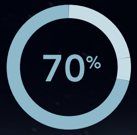
The risk of not addressing your domain security can be catastrophic. Domains that are not being protected pose a significant threat to your cyber security posture, data protection, consumer safety, intellectual property, supply chains, revenue, and reputation.

CSC recommends paying close attention to the following cyber risk framework for domain security:

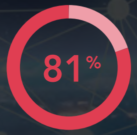
DOMAIN SECURITY FRAMEWORK


Protect against suspicious and malicious domains
Safeguard against email header spoofing
Defend against compromised domain activity

KEY FINDINGS FROM RESEARCH



70% of homoglyph domains (fuzzy matches)—a tactic commonly used in phishing and brand abuse—are owned by third parties and registered with consumer-grade registrars. Of these domain registrations, over 60% have been registered in the last two years, which demonstrates that this is an accelerating attack method.



81% are at greater risk of domain name and domain name system (DNS) hijacking because they have NOT adopted basic domain security measures like the domain registry lock protocol.

57% are relying on consumer-grade domain registrars with limited protection against domain and DNS hijacking, distributed denial of service (DDoS), man-in-the-middle attacks (MitM), or DNS cache poisoning.

Only 50% are using Domain-based Message Authentication, Reporting, and Conformance (DMARC) records as an email authentication method.

Importance of domain security in mitigating phishing

Recent cyber attacks have targeted connected supply chains in vital industries and across software platforms, where one compromise equates to exponential returns. Due to the interconnected nature of domains and DNS, the stated domain security and domain registrar vulnerabilities can result in further risk to the internet supply chain. Proactive, preventative controls can secure the underlying domain assets and defend against the aforementioned phishing attack methods. Must-haves include:

- **Domain registrar standards** that educate on the pitfalls of large organizations using consumer-grade registrars and prevent business practices that are used for malicious purposes such as phishing and brand abuse.
- **Industry-wide adoption of domain security measures** such as domain registry locks, DMARC, DNS hosting redundancy, DNS security extensions (DNSSEC), and certificate authority authorization (CAA) records.
- **Ongoing rapid detection and de-activation of confusingly similar domains** imitating brands, which are being used for phishing and other fraudulent activity.

Domain security:

Suspicious or malicious domain activity targeting the Global 2000

We identified and analyzed domains containing the brand names with more than six characters from the Global 2000 companies that were not owned by the brands themselves[1]. The intent of these suspicious or malicious domain registrations is to leverage the trust placed on the targeted brand to launch phishing attacks or other forms of digital brand abuse or IP infringement that leads to revenue loss, traffic diversion, and a diminished brand reputation.

There are endless domain-spoofing tactics and permutations that can be used by phishers and malicious third parties.

DOMAIN SPOOFING TACTICS

Fuzzy matches
cscg1obal.com
cscgl0bal.com

Homoglyphs – IDNs
ćscglobal.com
csçglobal.com

Cousin domains
cscglobal.jp
cscglobal.ec

Keyword match
cscglobalcovid.com
covidcscglobal.ar
covid19.com

Homophones (Soundex)
siesiglobal.com
cscclobol.com

We chose to focus our domain security research on one of many blatant tactics targeting the core brands of the Global 2000 companies with malicious domain registration activity.

Common homoglyphs (fuzzy matches) in .COM domains

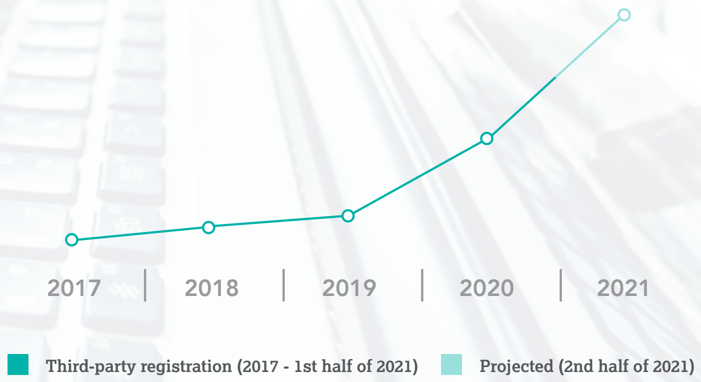
Based on frequent observation of use in phishing domains, our analysis included common Latin-character substitutions, for example, using C0rnpanyNarne.com to look like CompanyName.com.

C0rnpanyNarne.com

Most popular character substitutions

i → l	m → rn	i → 1	s → 5
o → 0	e → 3	l → 1	l → i

Global 2000 third-party homoglyph domain registrations



[1] The scope of the research was limited to the .COM extensions where we expected to find most third-party registrations. We took a conservative and meaningful approach to avoid any false positives and we analyzed core brands with six or more characters.

70% of the registered domains that resembled the Global 2000 brands were owned by third parties.

Out of the third-party owned domains:

60% were registered from 2020 through the first half of 2021. We project that by the end of 2021, this may be as high as **68%** based on our forecast.

77% used domain privacy services, or also had WHOIS details redacted.

This demonstrates the attempt to mask or hide their ownership and identity, showing they may have some nefarious intentions. As a point of reference, legitimate brands from the Global 2000 use privacy services or had their details redacted only 25% of the time.

43% are configured with MX (email) records.

Close to half of these domains are configured with MX records that can be used to send phishing emails or to intercept email.

Domain registrars most associated with suspicious or malicious, third-party owned registrations in the analysis:

- **GoDaddy.com, LLC**
- **Namecheap, Inc**
- **PDR, Ltd**

How are these third-party domains currently being used?

56% are pointing to advertising, pay-per-click web content, or are being used for domain parking.

Palo Alto's research shows how pay-per-click domains are used to spread malware via these services. Cyber criminals can use dormant domains as a strategy, and turn them on just when they're ready to attack.

38% had inactive websites.

Of these domains, 1/3 do not have nameservers associated with them. This may indicate that the domain name was suspended at some point.

Of the remaining 2/3, **57%** have active MX records.

6% were pointed toward brand impersonation and malicious content including phishing and potential malware delivery.

Undesirable content could damage a brand's reputation and customer confidence. The risk is that the user could engage with websites that contain malicious content or attempt to steal sensitive information.

Recommendations

From the analysis of these domains owned by third parties, many have a high propensity to be used as malicious domains for cyber attacks. The registrants typically hide behind privacy services or redacted WHOIS to mask their identities, register domains that look confusingly similar to known brands, and use tactics to look legitimate to entice an end user to click on a link, or trust a site that is infringing on a brand.

We recommend that companies establish a robust domain, web, and phishing monitoring program coupled with takedown capabilities. They should also establish a secure 360-degree domain management strategy to register exact matches, protect against a variety of domain spoofing tactics such as homoglyphs, fuzzy matches, cousin domains, as well as register across new generic top-level domains (gTLDs) and country code domain extensions associated with countries of operations and sales, in addition to other high-risk countries and extensions.

Domain security analysis

The domain name security posture of the Forbes Global 2000

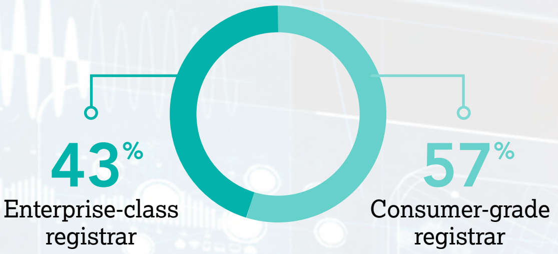
The insights shared in this report are based exclusively on publicly available data sets, all of which are easily accessible to cyber criminals and state-sponsored actors to facilitate DNS attacks and domain name hijacking. Therefore, it's our intent to elevate the awareness of these threats and share our domain security best practices to improve all organization's domain security posture. In this analysis, CSC looked at the adoption of the domain security measures outlined below across the Global 2000 list, and then we performed a deep dive into the industry groups and regions.

In this year's report, we also analyzed the trend of domain security adoption with respect to the type of domain registrar used. Across all security controls, we observed greater adoption among companies that use enterprise-class registrars compared to those using consumer-grade ones. This is especially apparent for the adoption of registry locks, as most consumer-grade registrars do not support such registry locks.

On average, the adoption of domain security controls is two times higher for enterprise-class registrars than for those using consumer-grade registrars.

Our observations are based on the companies included in the Global 2000. For 2020, the companies analyzed differ slightly from last year because companies move on and off the list each year.

Domain registrar provider



FINDINGS

57% of the Global 2000 companies—the largest public companies in the world—are not using enterprise-class registrars. The management of the overall domain name portfolio by a reputable enterprise-class registrar versus a consumer-grade registrar will make the adoption of domain security standards and best practices possible.

KEY COMPONENTS OF AN ENTERPRISE-CLASS REGISTRAR:

☑ Enterprise-wide scale and expertise with a corporate-only domain DNS and certificate management offering.

☑ Mission and focus on cyber security and IP protection.

Do not provide:

- Domain services through retail websites or reseller offerings
- Pay-per-click, domain spinning, and domain auctioning services that facilitate the infringement of intellectual property and trademarks

☑ Emphasis on domain security via advanced services such as: domain registry lock, DMARC, DNSSEC, CAA records, and DNS hosting redundancy.

☑ Provide global and local 24x7x365 support capabilities with worldwide domain registration capabilities.

☑ Implementation of Know Your Customer (KYC) methods of sourcing and validating client interactions.

☑ Internet Corporation for Assigned Names and Numbers (ICANN) and registry accredited globally.

☑ Offer domain, brand and fraud monitoring and enforcement and takedown capabilities.

☑ Offer complimentary advisory services and tools (i.e., CSC Security Center^{SM}) that facilitate domain management and security along with brand and fraud protection.

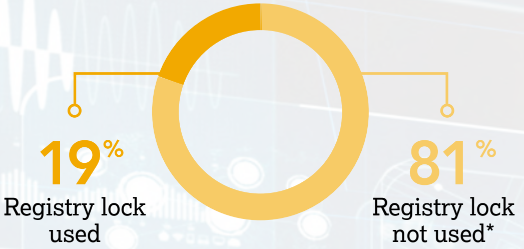
☑ Use best-in-class operations processes and controls such as mandating written requests, conducting cyber security awareness training, and taking data and policy measures.

☑ Have best-in-class operations practices that put security at the forefront of its mission, including ISO 27001 accredited data centers, SOC 2 compliance, and third-party penetration and vulnerability testing.

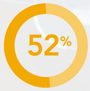
THREAT

Historically, consumer-grade registrars have been a frequent target for cyber attacks. An overwhelming number enable brand abuse and fraud. (See above for reasons to use an enterprise-class domain registrar.)

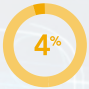
Registry lock



Use by registrar type



of companies that work with an enterprise-class registrar use registry lock



of companies that work with a consumer-grade registrar use registry lock

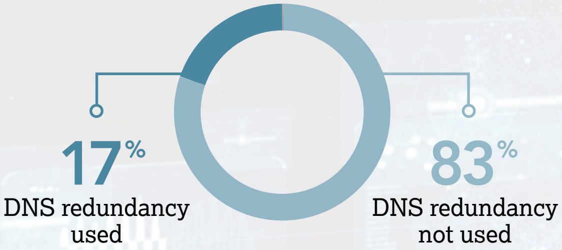
FINDINGS

Alarmingly, only 19% use registry lock as a security measure, signaling that four out of five Global 2000 companies are highly compromised in terms of domain security. Based on continued DNS hijacking risks against global businesses, this is very low adoption of this control by Global 2000 companies. Among the 43% of Global 2000 companies that use enterprise-class registrars, there's a higher percentage of 52% adopting registry locks versus only 4% among companies that use consumer-grade registrars. This suggests that the type of registrar used influences the adoption of domain security controls.

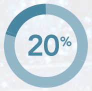
THREAT

A registry lock enables end-to-end domain name transaction security to mitigate human error and third-party risk. It's a highly cost-effective means to protect domain names against accidental or unauthorized modifications or deletions. Unlocked domains are vulnerable to social engineering tactics, which can lead to unauthorized DNS changes and domain name hijacking. *Also, some domains may remain unlocked, as not every registry around the world offers lock services.

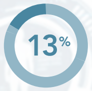
DNS redundancy



Use by registrar type



of companies that work with an enterprise-class registrar have implemented DNS redundancy



of companies that work with a consumer-grade registrar have implemented DNS redundancy

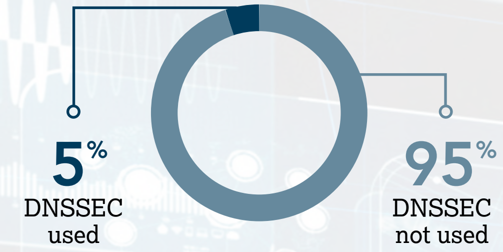
FINDINGS

Only 17% of Global 2000 companies have DNS redundancy for their core domain (secondary DNS). Over 80% are taking a risk not having secondary DNS, which would mitigate threats that could become costly incidences if employees or customers are unable to access or transact on their websites for even a few minutes.

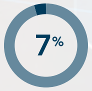
THREAT

Lack of DNS redundancy poses potential security threats like reduced resiliency to DDoS attacks, as well as down time. These attacks flood your network, service, or application, preventing real customer requests from getting through, leading to revenue loss and diminished reputation.

DNSSEC



Use by registrar type



of companies that work with an enterprise-class registrar use DNSSEC

of companies that work with a consumer-grade registrar use DNSSEC

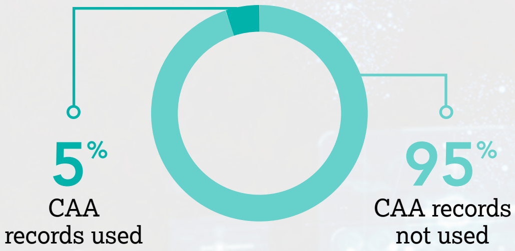
FINDINGS

Domain name system security extensions (DNSSEC) is another method to enable authenticated communication between DNS servers. Adoption rates for DNSSEC are very low at only 5%. DNSSEC prevents DNS cache poisoning attacks from occurring. This means 95% of all Global 2000 companies are prone to a cache poisoning attack.

THREAT

Lack of deployment of DNSSEC—one of the most cost-effective security protocols—leads to vulnerabilities in the DNS, which could include an attacker hijacking any step of the DNS lookup process. As a result, hackers can take control of an internet browsing session and redirect users to deceptive websites.

CAA records



Use by registrar type

of companies that work with an enterprise-class registrar use CAA records

of companies that work with a consumer-grade registrar use CAA records

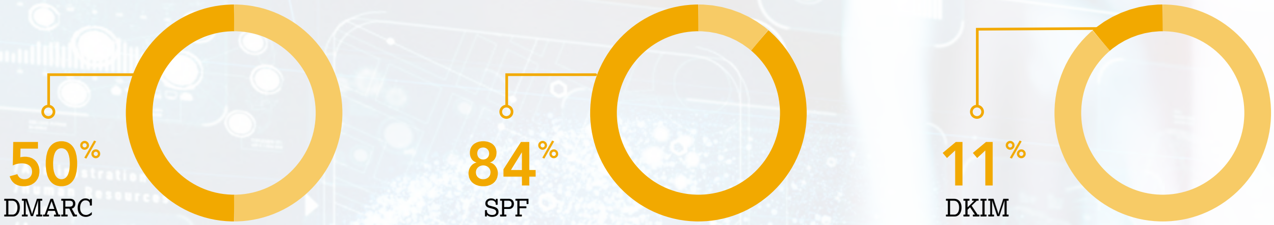
FINDINGS

Only 5% of Global 2000 companies use certificate authority authorization (CAA) records. CAA records allow you to designate a specific certificate authority (CA) to be the sole issuer of certificates for your company's domains. If a cyber criminal doesn't use the appointed certificate authority to get a new certificate, their request will fail, and you'll receive an alert that someone tried to request a new certificate outside of your CAA policy. This is a great compliance tool, and also a great security layer.

THREAT

Once a cyber criminal gets access to a domain name, in many cases they will gain access to digital certificates issued. By adding CAA records, it ensures that only your chosen provider can issue a certificate for your domain names, and is an essential technical control allowing for policy enforcement and mitigating cyber threats like HTTPS phishing of hijacked sub domains.

Email authentication



Use by registrar type

70% of companies that work with an enterprise-class registrar use DMARC

44% of companies that work with a consumer-grade registrar use DMARC

FINDINGS

Domain-based message authentication, reporting, and conformance (DMARC) use is now at 50% for the Global 2000 companies. DMARC is an email validation system designed to protect a company's email domain from being used for email spoofing, phishing scams, and other cyber crime. DMARC essentially provides email authentication the same way DNSSEC does at the DNS level. We also know that even with DMARC records in place, not having a DMARC reject policy still poses phishing risks.

THREAT

It's very easy to spoof email and make it look like it's being sent from a legitimate source when it really isn't. Authenticating the email channel with DMARC, SPF, or DKIM minimizes the incidence of email spoofing and potential phishing.

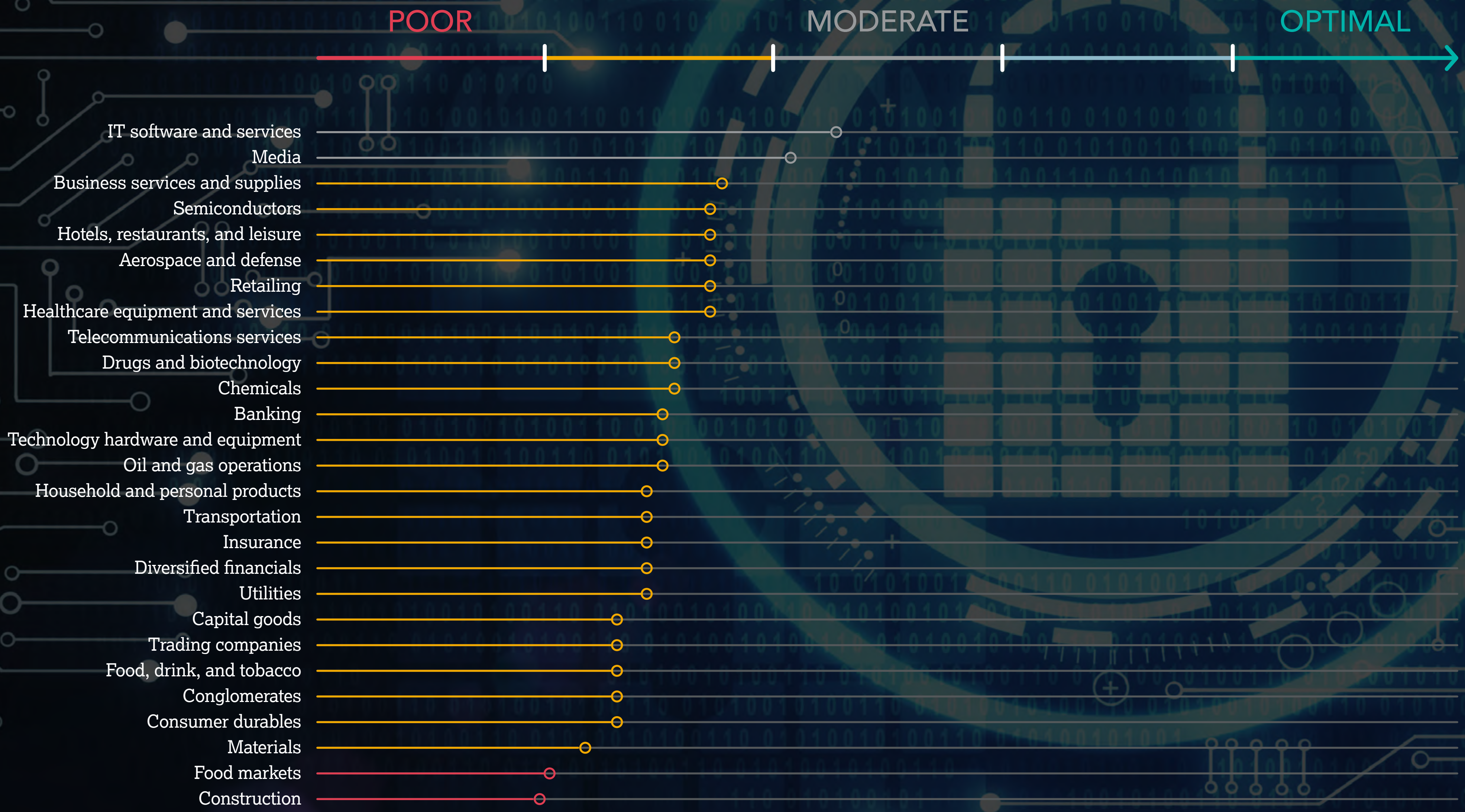
Domain name security controls adoption by industry groups

Some industries have found themselves more in the spotlight because of COVID-19. Those industries are healthcare equipment and services, drugs and biotech, chemical, and household and personal products. The increased demand on all of these industries over the past year and a half have made them key targets for cyber criminals. So it's highly concerning that these industries still appear in the middle-to-lower half of the risk mitigation effectiveness scale. Across these four industries, there is extremely low adoption of DNSSEC, with healthcare equipment and services, and household and personal products at 0% adoption. CAA records are similarly not well adopted, meaning that compromised domains could have digital certificates applied to them to give the impression of legitimacy, without the brand's knowledge. Also, on average, only one in four organizations within these industries adopt registry locks, which prevents domain name hijacking and unauthorized changes to DNS. But perhaps the low adoption of these three protocols is not surprising, considering 32-48% of companies within these industries are using consumer-grade registrars, which do not offer DNSSEC, registry locks, or CAA records as standard. So additionally, they could benefit from choosing to work with an enterprise-class domain registrar.

Also in the spotlight recently is the oil and gas industry, especially since the U.S. energy company Colonial Pipelines' ransomware attack, which forced the shutdown of 5,500 miles of its interstate fuel pipeline. "The incident is one of the most disruptive digital ransom operations ever reported and has drawn attention to how vulnerable U.S. energy infrastructure is to hackers," commented Reuters. Companies in the oil and gas industry should take serious note of this—especially as our statistics show that in the Global 2000, the oil and gas industry appears in the bottom half of the effectiveness scale. Just 4% of companies in this industry use DNSSEC, and 10% use registry lock.

The banking sector remains a mixed bag in terms of domain and DNS security adoption. This said, for an industry that is arguably the prime target for phishing attacks, a 49.7% adoption of DMARC—the email authentication protocol—is still worryingly low.

Risk mitigation effectiveness scale



Recommendations

Domain security is the missing link in most cyber security strategies. Having best-in-class security measures for your domains can help to prevent phishing attacks, BEC, and ransomware attacks in their early stages. Many industry experts have emphasized that it's very important to maintain strong cyber hygiene. Domain security is a prime example where companies are falling short. Domain security plays a preventative role in phishing attacks, which then would also prevent BEC attacks, impersonation fraud, ransomware attacks, and many other threats.

All companies in all industries—and especially those more exposed now due to COVID-19—should adopt a multi-layer defense-in-depth approach for domain security, starting with working with an enterprise-class provider. CSC recommends four key strategies:

Adopt a defense-in-depth approach for domain management

Confirm that your domain registrar's business practices are not contributing to fraud and brand abuse

Continuously monitor the domain space and key digital channels like marketplaces, apps, social media, and email for brand abuse, infringements, phishing, and fraud

Leverage global enforcement, including takedowns and advanced techniques in internet blocking

ADOPT A DEFENSE-IN-DEPTH APPROACH FOR DOMAIN MANAGEMENT

- Eliminate your third-party risk by assessing your domain registrar's security, technology, and processes along with your DNS management provider
- Secure vital domain names, DNS, and digital certificates through:
  - Implementing two-factor authentication
  - Monitoring DNS activity
  - Using security measures like domain registry locks, DNSSEC, DMARC, CAA records, and redundancy on DNS hosting

CONFIRM THAT YOUR DOMAIN REGISTRAR'S BUSINESS PRACTICES ARE NOT CONTRIBUTING TO FRAUD AND BRAND ABUSE

The following issues are often common with consumer-grade domain registrars:

- Operating domain marketplaces that drop catch, auction, and sell domain names containing trademarks to the highest bidder
- Domain name spinning and advocating the registration of domain names containing trademarks
- Monetizing domain names containing trademarks with pay-per-click sites
- Frequently occurring breaches resulting in DNS attacks, phishing, and BEC

CONTINUOUSLY MONITOR THE DOMAIN SPACE AND KEY DIGITAL CHANNELS LIKE MARKETPLACES, APPS, SOCIAL MEDIA, AND EMAIL FOR BRAND ABUSE, INFRINGEMENTS, PHISHING, AND FRAUD

- Leverage phishing monitoring and a fraud-blocking network of browsers, partners, ISPs, and SIEMs
- Identify domain and DNS spoofing tactics such as homoglyphs (fuzzy matches and IDNs), cousin domains, keyword match, and homophones
- Identify trademark and copyright abuse on web content
- Protect your brands from abuse on online marketplaces through marketplace monitoring
- Track all mentions of brands across relevant social media channels
- Monitor the major app stores
- Find the ads that cost you traffic and damage your brand

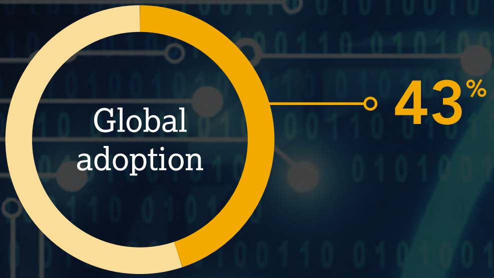
LEVERAGE GLOBAL ENFORCEMENT, INCLUDING TAKEDOWNS AND ADVANCED TECHNIQUES IN INTERNET BLOCKING

- Use a combination of actions to enforce on IP infringements and fraud:
  - Primary enforcement actions include marketplace delistings, social media page suspensions, mobile app delistings, cease and desist letters, fraudulent content removal, and complete threat vector mitigation
  - Secondary enforcement actions include registrar-level domain suspensions, invalid WHOIS domain suspensions and fraud alerting
  - Tertiary enforcement actions include Uniform Domain-Name Dispute-Resolution Policy and Uniform Rapid Suspension procedures, domain acquisitions, in-depth investigations, and test purchasing
- Use a range of technical and legal approaches for enforcement, selecting the most appropriate approach case by case

Industry adoption by security measure

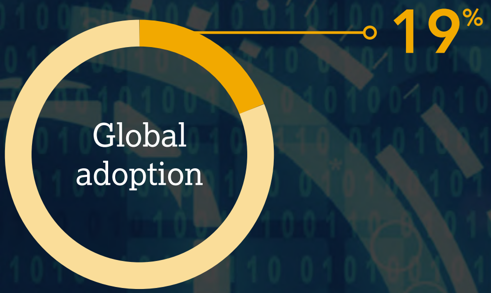
○ HIGH ADOPTION ○ LOW ADOPTION

Enterprise-class domain registrar



Hotels, restaurants, and leisure	75%
Household and personal products	68%
Business services and supplies	65%
Media	64%
IT software and services	61%
Chemicals	57%
Retailing	56%
Drugs and biotechnology	56%
Aerospace and defense	54%
Semiconductors	53%
Healthcare equipment and services	52%
Capital goods	47%
Transportation	47%
Food, drink, and tobacco	47%
Consumer durables	46%
Insurance	45%
Technology hardware and equipment	42%
Banking	38%
Conglomerates	38%
Telecommunications services	36%
Trading companies	35%
Diversified financials	35%
Utilities	35%
Oil and gas operations	28%
Construction	24%
Materials	22%
Food markets	22%

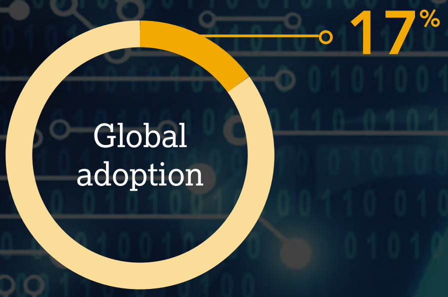
Registry lock



IT software and services	48%
Media	40%
Aerospace and defense	33%
Business services and supplies	33%
Semiconductors	28%
Telecommunications services	28%
Retailing	27%
Chemicals	27%
Drugs and biotechnology	27%
Healthcare equipment and services	25%
Consumer durables	24%
Capital goods	23%
Hotels, restaurants, and leisure	21%
Household and personal products	21%
Diversified financials	20%
Transportation	19%
Technology hardware and equipment	19%
Insurance	18%
Food, drink, and tobacco	16%
Banking	14%
Conglomerates	13%
Utilities	11%
Oil and gas operations	10%
Materials	9%
Food markets	6%
Construction	6%
Trading companies	3%

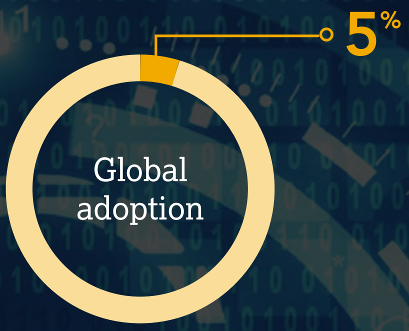
○ HIGH ADOPTION ○ LOW ADOPTION

DNS redundancy



Transportation	28%
Oil and gas operations	25%
Banking	23%
IT software and services	23%
Aerospace and defense	21%
Trading companies	21%
Telecommunications services	20%
Chemicals	20%
Semiconductors	19%
Insurance	19%
Retailing	18%
Diversified financials	17%
Hotels, restaurants, and leisure	17%
Food markets	16%
Capital goods	14%
Consumer durables	13%
Materials	12%
Business services and supplies	12%
Media	12%
Household and personal products	12%
Utilities	11%
Drugs and biotechnology	11%
Food, drink, and tobacco	10%
Construction	9%
Conglomerates	9%
Technology hardware and equipment	8%
Healthcare equipment and services	7%

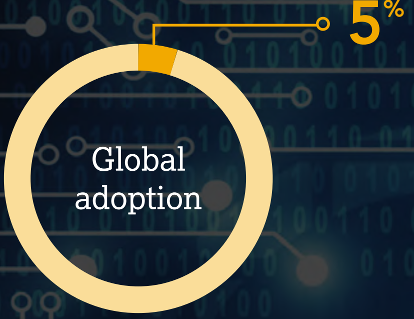
DNSSEC



IT software and services	14%
Aerospace and defense	13%
Media	12%
Banking	9%
Semiconductors	9%
Diversified financials	6%
Utilities	6%
Business services and supplies	6%
Insurance	4%
Telecommunications services	4%
Oil and gas operations	4%
Capital goods	4%
Consumer durables	3%
Trading companies	3%
Drugs and biotechnology	3%
Construction	2%
Chemicals	2%
Technology hardware and equipment	2%
Hotels, restaurants, and leisure	0%
Healthcare equipment and services	0%
Retailing	0%
Transportation	0%
Household and personal products	0%
Food, drink, and tobacco	0%
Conglomerates	0%
Materials	0%
Food markets	0%

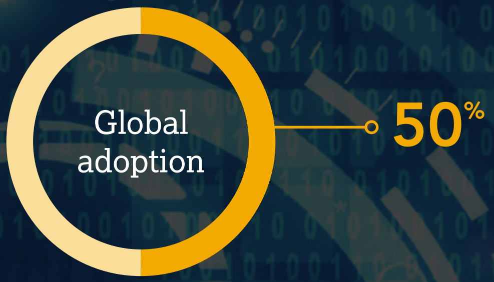
○ HIGH ADOPTION ○ LOW ADOPTION

CAA records



Media	16%
IT software and services	13%
Oil and gas operations	13%
Banking	9%
Business services and supplies	8%
Telecommunications services	8%
Conglomerates	6%
Utilities	6%
Diversified financials	6%
Chemicals	5%
Technology hardware and equipment	5%
Healthcare equipment and services	5%
Hotels, restaurants, and leisure	4%
Transportation	4%
Insurance	4%
Materials	3%
Retailing	3%
Drugs and biotechnology	3%
Consumer durables	2%
Capital goods	2%
Construction	1%
Food, drink, and tobacco	1%
Semiconductors	0%
Aerospace and defense	0%
Household and personal products	0%
Trading companies	0%
Food markets	0%

DMARC



IT software and services	74%
Healthcare equipment and services	73%
Semiconductors	72%
Media	64%
Hotels, restaurants, and leisure	63%
Retailing	60%
Drugs and biotechnology	60%
Oil and gas operations	59%
Conglomerates	56%
Telecommunications services	56%
Technology hardware and equipment	56%
Food, drink, and tobacco	54%
Utilities	54%
Business services and supplies	53%
Aerospace and defense	50%
Banking	50%
Materials	47%
Household and personal products	47%
Transportation	46%
Insurance	46%
Diversified financials	43%
Trading companies	41%
Chemicals	41%
Consumer durables	38%
Food markets	38%
Capital goods	37%
Construction	28%

CSC

CSC is the trusted provider of choice for the Forbes Global 2000 and the 100 Best Global Brands® in the areas of enterprise domain names, domain name system (DNS), digital certificate management, as well as digital brand and fraud protection. As global companies make significant investments in their security posture, CSC can help them understand known security blind spots that exist and secure their domain names, DNS, and digital certificates. By leveraging our proprietary security solutions, CSC secures companies from cyber threats to their online assets, helping them avoid devastating revenue loss, brand reputation damage, or significant financial penalties as a result of policies like the General Data Protection Regulation (GDPR). We also provide online brand protection—the combination of online brand monitoring and enforcement activities—taking a holistic approach to digital asset protection, along with fraud protection services to combat phishing.

Research and editorial prepared by CSC

Vincent D'Angelo, global director, Corporate Development and Strategic Alliances

Stephanie Mitchell, manager, Marketing

Quinn Taggart, senior advisor, Global Brand Security

Letitia Thian, manager, Marketing

Sue Watts, global leader, Marketing

cscdbs.com

CSC is a service company and does not provide legal or financial advice. The materials here are presented for information purposes only.
Consult with your legal or financial advisor to determine how this information applies to you.