CSC

DOMAIN SECURITY REPORT:
FORBES GLOBAL 2000 COMPANIES

JUNE 2020

Executive Summary

The world has changed in 2020 with the COVID-19 pandemic currently wreaking havoc across the world. For most on our fragile planet, the focus has shifted to safeguarding our loved ones and ourselves by securing the basics of food, clothing, and shelter. There is a lot of uncertainty with our financial markets, the extent of causalities, and the long-term emotional and psychological impact to our society. The recovery will not be easy, but united as a global community, we will be stronger by working together.

Unfortunately, cyber criminals are not of the same mindset. They are leveraging this pandemic to launch dangerous cyber attacks, phishing, counterfeiting, and misinformation scams. They reference trusted brands and products, government agencies, and health organizations via fraudulent domain names, email, websites, apps, social media profiles, and marketplace listings.

This report shows that 83% of Global 2000 organizations are at greater risk of domain name hijacking, because they have NOT adopted basic domain security measures like the registry lock protocol, for those that offer it.

The dangers of unsecure, retail-grade domain name registrars

Increasingly, we are hearing about how retail domain name registrars have proven to be vulnerable to security threats, the latest being a data breach where a bad actor accessed customer login credentials, possibly affecting all 19 million company accounts[1].

This report shows that 53% of the Forbes Global 2000 use retail-grade registrars.

The difference between a retail registrar and an enterprise-class registrar lies within the level of technology controls, accreditation, and operations processes that are in place. From a technology standpoint, having Tier 4 data centers, being ISO 27001/2 compliant, performing continual vulnerability assessment and penetration testing, and 24x7 monitoring response can make a real difference. Equally as important is using an Internet Corporation for Assigned Names and Numbers (ICANN) and registry-accredited provider, and to have the right operation processes in place to ensure that our customers' online assets are protected. Implementing a security first policy, phishing awareness, social engineering training, a mandated clear desk policy, and being data and General Data Protection Regulation (GDPR) compliant make a difference in the ability to secure against cyber threats.

Registry locks are critical, yet still so underused

Not to be overlooked are best practices to safeguard against domain name system (DNS) and domain name hijacking, including securing remote worker systems like virtual private networks (VPNs) and implementing domain name and DNS security.

Industry findings highlight inconsistent security

Findings by industry are important indicators to determine an individual company's maturity level.

The information technology, and media and entertainment industries rank as the top overall industry leaders in terms of their domain security posture.

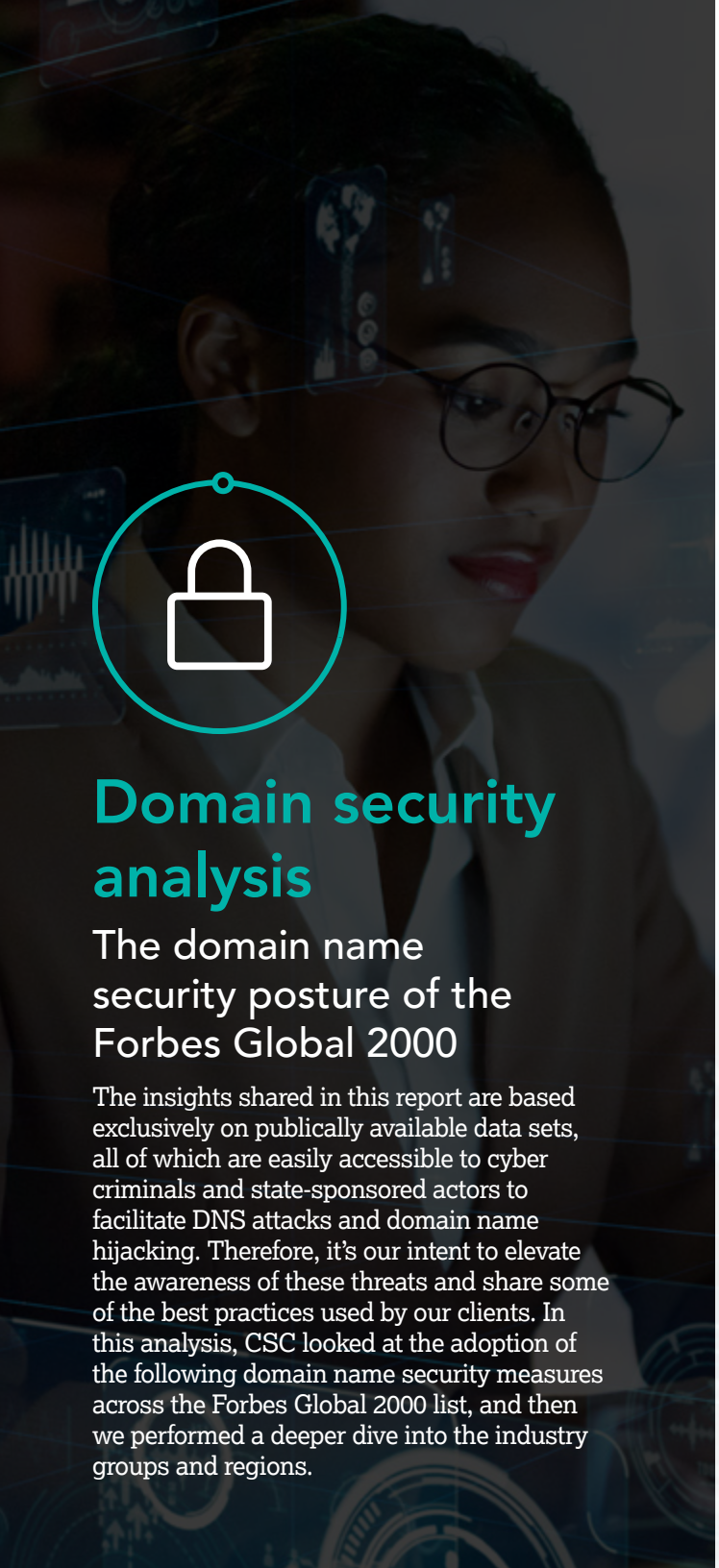
They also lead in the adoption of registry locks, domain-based message authentication reporting and conformance (DMARC), DNS security extensions (DNSSEC), and corporate registrar services, which are the keys to protecting against phishing, DNS, and domain name hijacking. This does not come as a surprise, as these industries have a natural disposition to implement stronger security countermeasures.

What surprised us was the weak security posture of banks that manage personally identifiable information (PII) and large amounts of money.

The banks in particular, show the lowest use of corporate domain registrar. One rationale may be because close to half of the banks represented in the Global 2000 are from Asia, and Asia is the region where there is clearly lower security measures in place.

Research and editorial prepared by CSC

Vincent D'Angelo, *global director, Corporate Development and Strategic Alliances*
Quinn Taggart, *senior domain product manager*
Sue Watts, *head of marketing*
Letitia Thian, *marketing manager*
Ken Linscott, *product director, Domains and Security*



Domain security analysis

The domain name security posture of the Forbes Global 2000

The insights shared in this report are based exclusively on publically 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 some of the best practices used by our clients. In this analysis, CSC looked at the adoption of the following domain name security measures across the Forbes Global 2000 list, and then we performed a deeper dive into the industry groups and regions.

Registry lock

Registry lock used

Registry lock not used

Registry lock unavailable*

THREAT

Unlocked domains are vulnerable to social engineering tactics, which can lead to unauthorized DNS changes and domain name hijacking. Some domains may remain unlocked, as not every registry around the world offers lock services*.

FINDINGS

Registry locks prevent domain name hijacking and unauthorized changes to DNS that could take a site offline or redirect users to malicious content. Based on continued DNS hijacking risks against global businesses, there is very low adoption of this control by Global 2000 companies.

Alarmingly, only 17% use it as a security countermeasure, signaling that four out of five Global 2000 companies are highly compromised in terms of domain security.

IN THE NEWS: DOES YOUR DOMAIN HAVE A REGISTRY LOCK?

A security expert lost his key domain to scammers even though he had a registrar lock, because his registrar succumbed to a scam, and transferred his domain to another registrar. This could have been prevented with a registry lock that prevents domain transfers initiated by the registrars, by requiring additional registry verification.

Domain registrar provider

THREAT

Historically, retail registrars have been frequent targets for cyber attacks. Companies should partner with an enterprise-class registrar that invests heavily in security at the technology level, as well as security training of employees, including instilling company values of vigilance, and knowing how to identify malicious intent, especially for core domains. In terms of threats to digital assets, the assets most at risk are those you don't yet know about, so consider ways to identify them, such as using a detective control like domain monitoring.

IN THE NEWS: PHISH OF GODADDY EMPLOYEE JEOPARDIZED ESCROW.COM, AMONG OTHERS

A spear phishing attack on the employee of one of the world's largest domain registrars gave attackers access to view detailed notes and information on its clients, and also the ability to modify the accounts' DNS records. The attacker had redirected a compromised client's site to a fraudulent page, and even obtained free digital certificates to encrypt it.

FINDINGS

53% of the Global 2000 companies—the largest public companies in the world—are not using enterprise-level registrars. The management of the overall domain name portfolio by a reputable corporate registrar versus a retail registrar will make the adoption of domain security standards much easier to implement and monitor. And there's three key components to being an enterprise-class provider:

1. **Technology:** Having enterprise-class Tier 4 data centers, being ISO 27001/2 compliant, performing continuous vulnerability assessment and penetration testing, and 24/7 monitoring response, to ensure that the provider's networks are protected and secure.
2. **Accreditation:** Being ICANN and registry accredited with all the top-level domains around the world, to be able to support global requirements in a consistent, secure manner.
3. **Operations:** Having the processes in place to make sure that customers' domains, DNS, and digital certificates are protected, by having a security-first policy, phishing awareness, and social engineering training, a mandated clear desk policy, working only with written requests, being data and GDPR compliant, so on and so forth.

DNS provider

Internal DNS | Enterprise DNS | Others

THREAT

Lack of DNS hosting redundancy and using non-enterprise-level DNS providers poses potential security threats like reduced resiliency to distributed denial of service (DDoS) attacks, as well as down time, and revenue loss.

FINDINGS

Only 20% of Global 2000 companies use enterprise-grade DNS hosting. Without having this, companies have increased exposure to DDoS attacks. There are numerous types of DDoS attacks that target DNS, including DNS amplification. These attacks flood your network, service, or application, preventing real requests from customers from getting through.

IN THE NEWS: BEYOND THE FIREWALL: DNS DEFENSES TO MANAGE ONLINE THREATS

The DNS forms the underlying infrastructure for how the internet works, serving as a directory to point users to the right web content. When DNS goes down, websites, email, voice-over IP, and remote employee login goes down with it.

DNSSEC

DNSSEC used | DNSSEC not used

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.

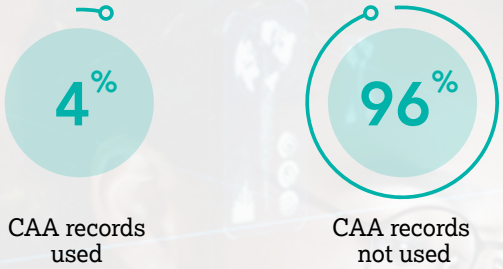
FINDINGS

DNSSEC is another method to enable authenticated communication between DNS servers. Adoption rates for DNSSEC are very low at only 3%. DNSSEC prevents DNS cache poisoning attacks from occurring. This means 97% of all Global 2000 companies are prone to a cache poisoning attack.

IN THE NEWS: DNSSEC SIGNING POTENTIALLY INTERRUPTED BY CORONAVIRUS

DNSSEC adds an additional level of security to the DNS. “Since these keys are critical to the infrastructure of the internet, there is a ceremony involved in regenerating these root keys, including multiple people and key material in locked safes that are live-streamed to ensure that there aren’t any compromises of data. These happen every three months and thus require regular meetings at the key signing sites with people from different countries to ensure that DNSSEC continues to operate.” However, with global restrictions on travel due to the ongoing coronavirus crisis, the keys will not be regenerated in time, and changes to normal procedures will be needed to keep the DNSSEC operating after June 2020.

CAA records



CAA records used

CAA records not used

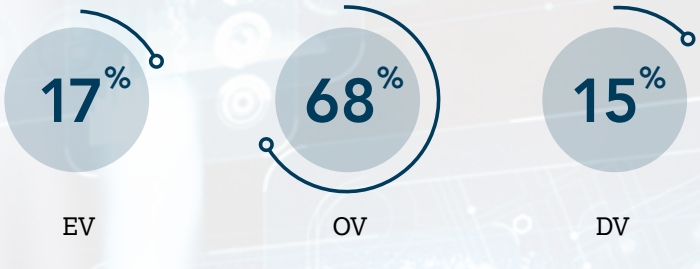
THREAT

A certificate authority authorization (CAA) record is a resource record held on a zone file that allows the domain owner to indicate which certificate authorities (CAs) are authorized to issue a certificate for a given domain name. By adding CAA records, you're able to control the CAs that your company uses. 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.

FINDINGS

When we looked at CAA records for the Global 2000, only 4% of the companies have them. Once a cyber criminal gets access to a domain name, they will then, in many cases, gain access to or have a new digital certificate issued. CAA records allow you to designate a specific certificate authority to be the sole issuer of certificates for your company's domains. So if the attacker doesn't go to that certificate authority to get a new certificate, their request will fail. Moreover, an alert will be sent to you to let you know that someone tried to request a new certificate that was outside of the CAA policy. This is a great compliance tool, but it's also a great security layer to know if someone is trying to issue a certificate on one of your key domain names.

Digital certificate validation



EV

OV

DV

THREAT

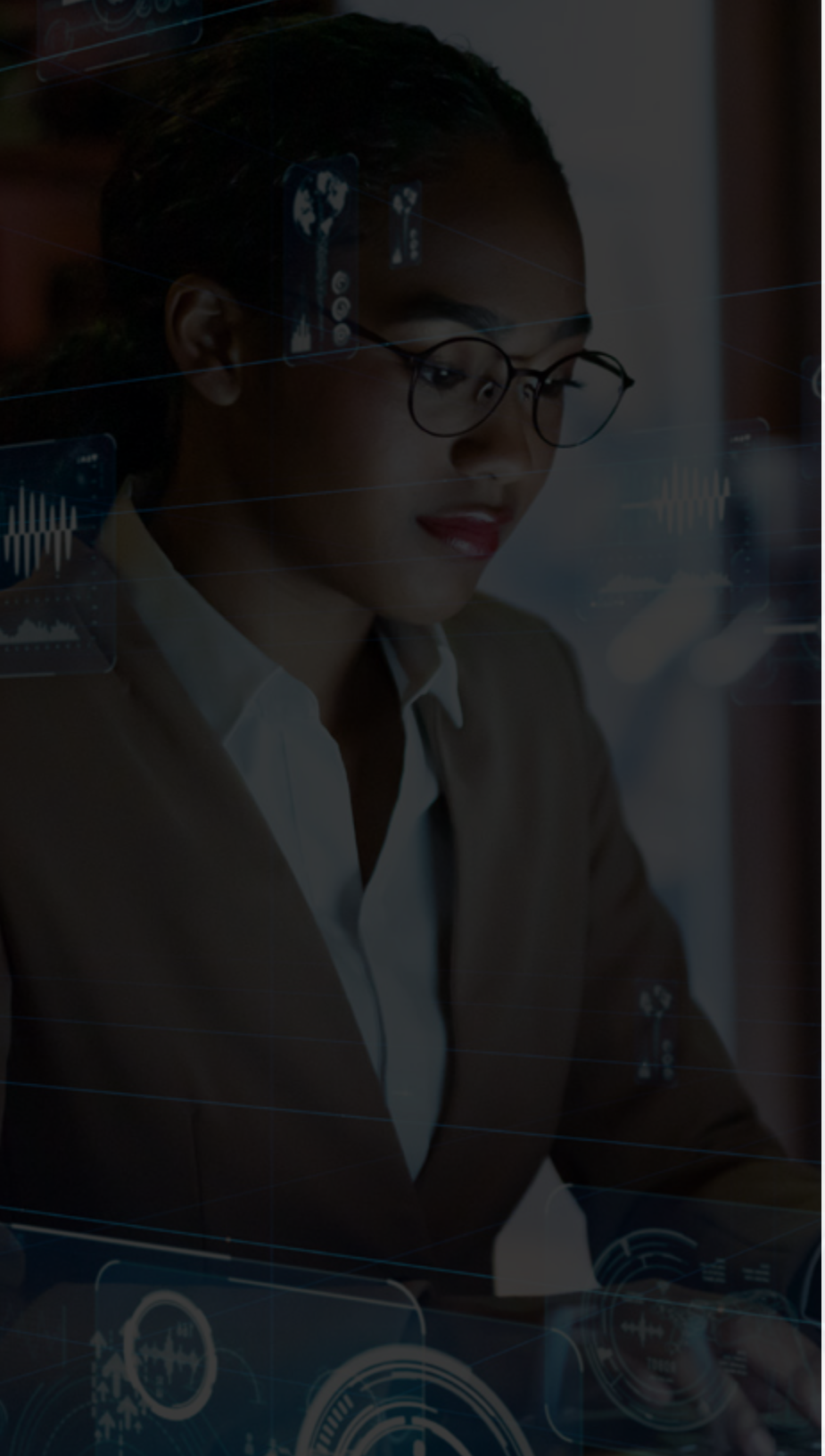
Digital certificate types that require more authentication, such as extended validation (EV) and organization validation (OV), are less prone to compromise than domain validation (DV).

FINDINGS

15% of Global 2000 companies are still just using DV certificates, which are more prone to compromise. If DNS is the door to a home, a digital certificate is the lock. It doesn't matter how solid the door is if the lock is weak. A key risk factor lies in the way in which digital certificates are validated. In the case of these companies, 85% are using certificates with higher levels of authentication.

IN THE NEWS: THE LIFE CYCLE OF DIGITAL CERTIFICATES REDUCES AGAIN

From September 1, 2020 onwards, browsers will only trust certificates that are no older than a year. The rationale to reduce lifetimes is that by having to replace certificates more frequently, businesses will increase the level of security through this recurring validation process, and be quicker to adopt more secure certificates. However, this will increase administration, and companies need to be prepared to manage shorter digital certificate lifetimes, or risk business disruption and security during a potential outage due to expired certificates.



Email authentication

THREAT

It is 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, sender policy framework (SPF), or domain keys identified mail (DKIM) minimizes the incidence of email spoofing and potential phishing.

FINDINGS

DMARC use is only at 39% 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. So whether you are using DMARC, SPF, or DKIM, these are effective in preventing email spoofing.

IN THE NEWS: WHY CORONAVIRUS SCAMMERS CAN SEND FAKE EMAILS FROM REAL DOMAINS

A scam email campaign soliciting donations with the intent for personal profit was sent using the legitimate domain name of World Health Organization (WHO). Such domain spoofing can be prevented by setting a DMARC policy for email authentication.

Domain name security controls adoption: by industry groups

● LOW ADOPTION ● HIGH ADOPTION

REGISTRY LOCK USED

GLOBAL ADOPTION	17%
MEDIA AND ENTERTAINMENT	40%
INFORMATION TECHNOLOGY	35%
HEALTHCARE	26%
CONSUMER DURABLES AND APPAREL	24%
HOTELS, RESTAURANTS, AND LEISURE	22%
DIVERSIFIED FINANCIALS	21%
TELECOMMUNICATION SERVICES	21%
RETAILING	20%
COMMERCIAL AND PROFESSIONAL SERVICES	19%
AUTOMOBILES AND COMPONENTS	19%
HOUSEHOLD AND PERSONAL PRODUCTS	19%
INSURANCE	16%
TRANSPORTATION	14%
FOOD, BEVERAGE, AND TOBACCO	13%
CAPITAL GOODS	13%
BANKS	12%
REAL ESTATE	12%
UTILITIES	11%
ENERGY	10%
MATERIALS	8%

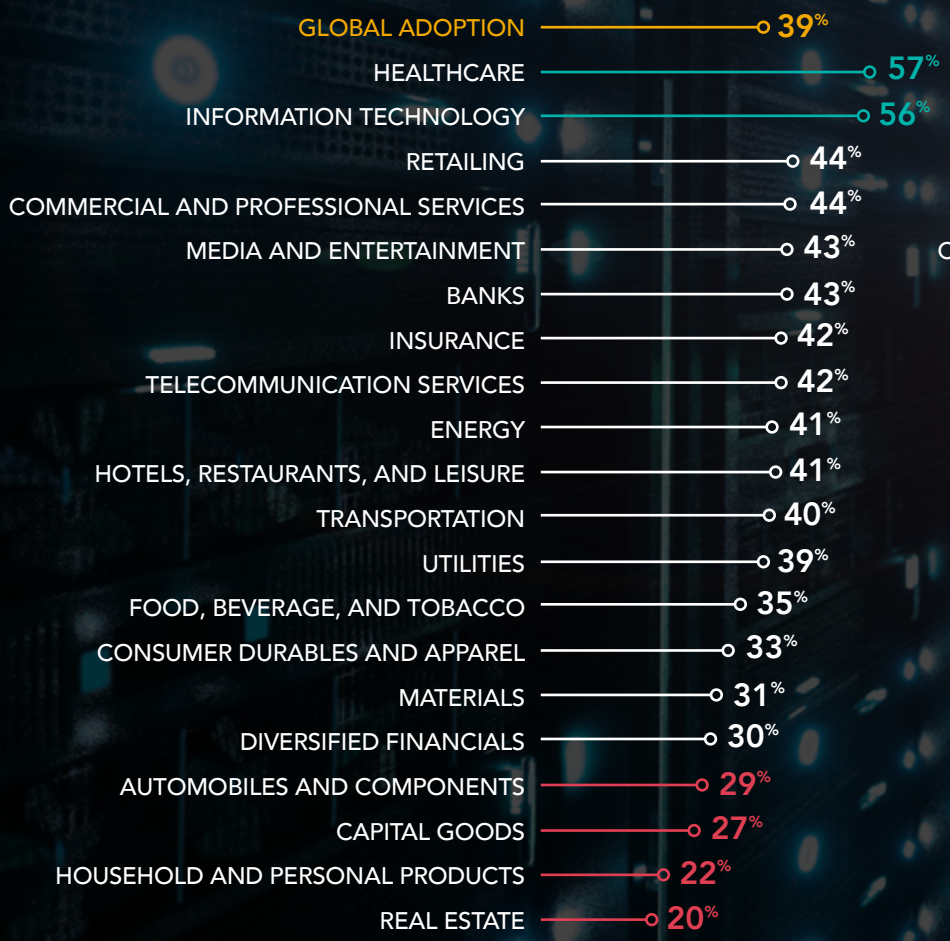
DNSSEC USED

GLOBAL ADOPTION	3%
MEDIA AND ENTERTAINMENT	7%
DIVERSIFIED FINANCIALS	6%
BANKS	5%
INFORMATION TECHNOLOGY	4%
TELECOMMUNICATION SERVICES	4%
UTILITIES	3%
CAPITAL GOODS	3%
ENERGY	2%
INSURANCE	2%
COMMERCIAL AND PROFESSIONAL SERVICES	2%
TRANSPORTATION	1%
MATERIALS	1%
REAL ESTATE	1%
HEALTHCARE	1%
AUTOMOBILES AND COMPONENTS	0%
CONSUMER DURABLES AND APPAREL	0%
FOOD, BEVERAGE, AND TOBACCO	0%
HOTELS, RESTAURANTS, AND LEISURE	0%
HOUSEHOLD AND PERSONAL PRODUCTS	0%
RETAILING	0%

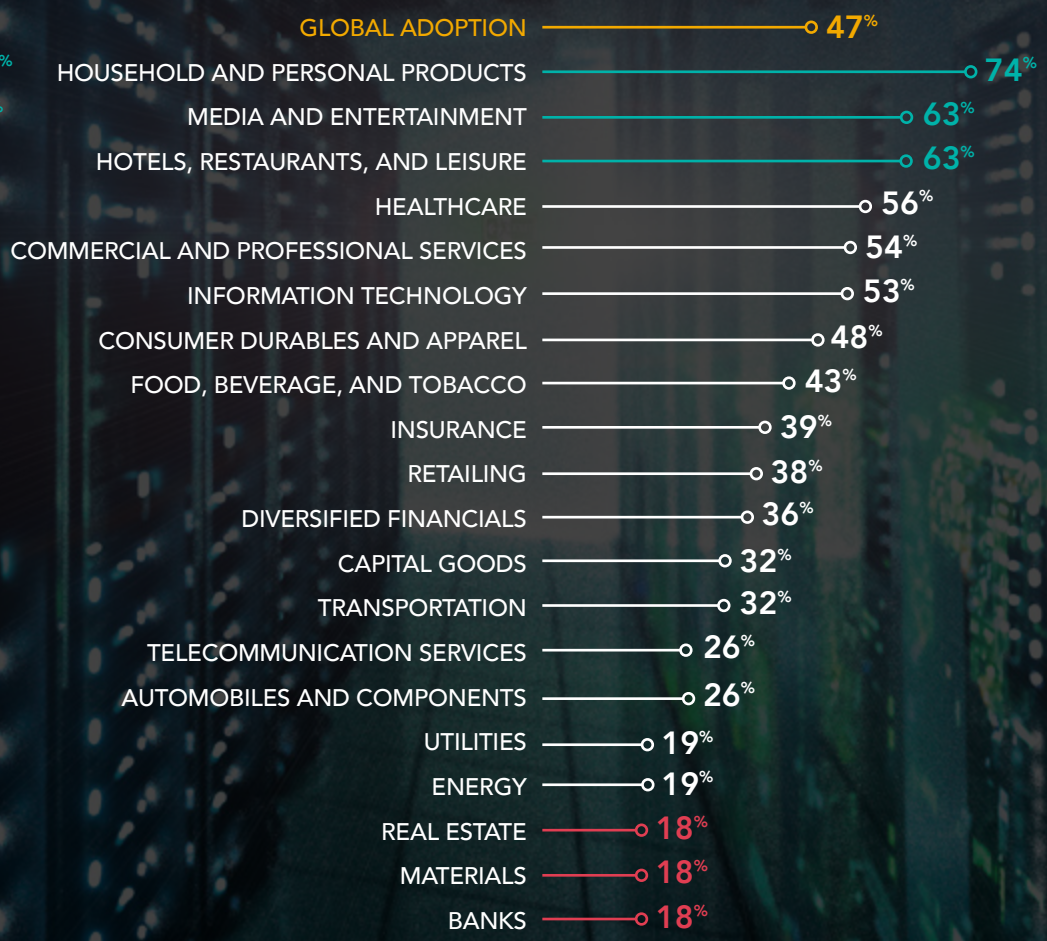
Domain name security controls adoption: by industry groups

● LOW ADOPTION ● HIGH ADOPTION

DMARC USED



CORPORATE DOMAIN REGISTRAR



The good, the bad, and the unexpected

Information technology, and media and entertainment rank as the top overall industry leaders in terms of their domain security posture. They also lead in the adoption of registry locks, DMARC, DNSSEC, and corporate registrar services, which are the keys to protecting against phishing, DNS, and domain name hijacking. This does not come as a surprise, as these industries have a natural disposition to implement stronger security countermeasures. The information technology companies in the Global 2000 list include major tech and security companies, hence show high adoption of online security protocol, therefore ranking #1.

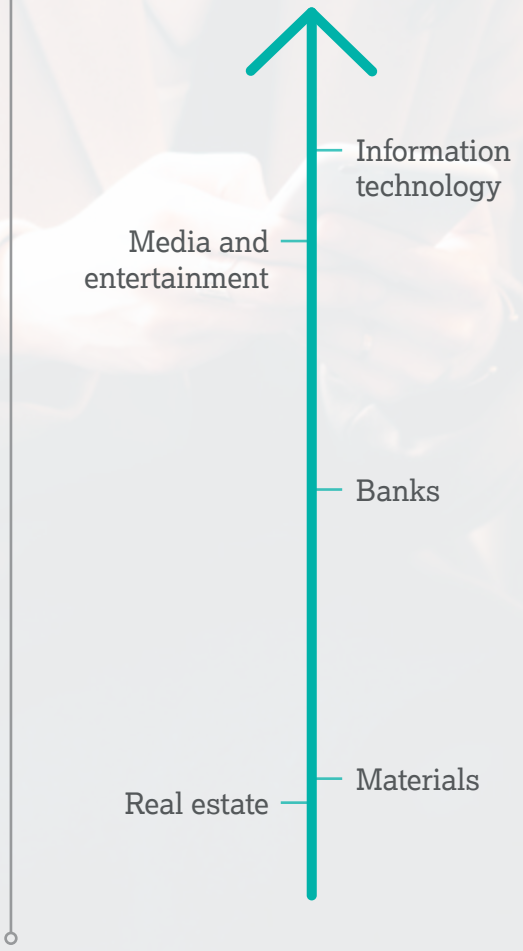
The media and entertainment industry comprise media conglomerates that own some of the biggest brand portfolios, as does the household and personal product industry, hence we observe the highest use of corporate domain registrars in these two industries, which is the most viable way for them to manage large, global portfolios of domain names.

As the media and entertainment industry pivot towards an online presence for distribution, we see corresponding high adoption rates for security controls such as registry locks for their main domains. A domain hijack that redirects their content to fraudulent websites would be detrimental to business. But the same import is not seen in the household and personal products industry, which may rely more heavily on partner channels for distribution.

The lowest ranking is the materials industry and real estate industries, showing low adoption of the four key security controls. The materials industry, that includes iron and steel industries, tends to have little online presence, which might explain their lack of adoption in domain security controls. However, we still believe there is much more they need to do to secure themselves, as they are just as susceptible to data breaches and phishing attacks as any industry.

What surprised us was the weak security posture of banks that manage PII and large amounts of money. The banks in particular, show the lowest use of corporate domain registrar. One rationale may be because close to half of the banks represented in the Global 2000 are from Asia. In our next section, we observe an undeniable trend that Asia-Pacific companies fare much lower in their security posture than their peers in the Americas and EMEA, hence explaining the skew in the banking industry.

DOMAIN SECURITY MATURITY SCALE



Domain name security controls adoption: by regions

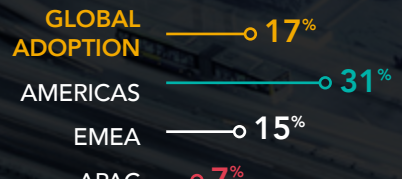
Americas leading the way

When observing domain name security adoption by region among the Global 2000 companies, the Americas rank #1, followed by EMEA at #2, and APAC at #3. The largest sector in the Americas is the information technology industry (11%), and as the industry leads in its security posture, it boosts the region's overall security posture. Another possible reason is the maturity of the region in its awareness for the various security controls available. Furthermore, many security compliance and protocols originate from the U.S., in contrast to Asia, which generally has fewer regulations.

APAC showed significantly lower adoption rates when compared to their peers in other regions. For example, the adoption of domain registry lock, and many other security controls was close to four times lower in APAC companies than those in the Americas. There is an observed positive correlation between the use of a corporate domain registrar and the use of other security controls such as registry locks, DNSSEC, DMARC, and CAA records. We think this explains the APAC region's weaker posture, as there are fewer corporate domain registrars in the APAC region.

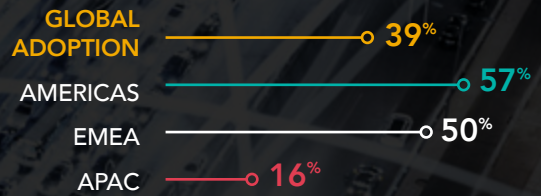
● LOW ADOPTION ● HIGH ADOPTION

REGISTRY LOCK USED

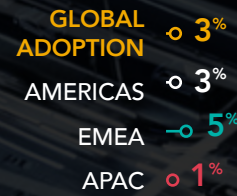


CORPORATE DOMAIN REGISTRAR

DMARC USED

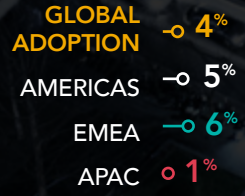


DNSSEC USED

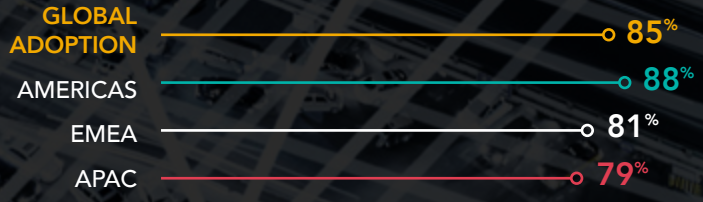


ENTERPRISE OR INTERNAL DNS

CAA RECORDS USED



DIGITAL CERTIFICATE VALIDATION (EV OR OV)

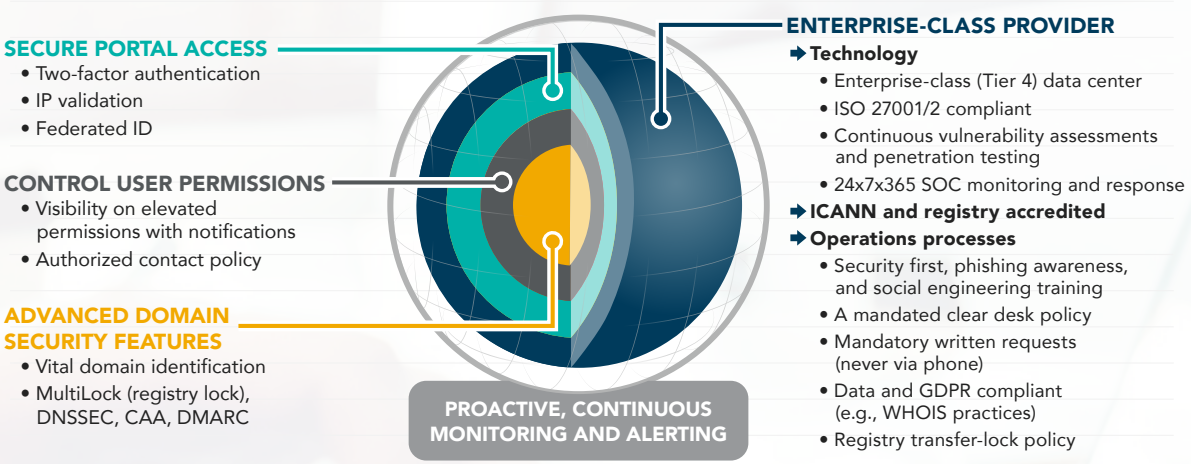


Recommendations

Companies have invested in security solutions at an exponential rate to protect themselves from continually evolving cyber security threats. In addition, while these investments are important, many companies remain vulnerable to what security experts are now referring to as critically important security blind spots.

Company domain names, DNS, and digital certificates are being attacked or compromised with increasing frequency, sophistication, and severity. These are all of the fundamental components of the most important applications that enable your company to conduct business—including your website, email, and more. Moreover, when they are compromised, criminals can redirect websites for financial gain, intercept email to conduct espionage, and even harvest credentials to breach your network. This can have a serious impact on your company's revenue and reputation and expose your company to significant financial penalties as a result of the EU's GDPR and other policies like it.

CSC recommends using a defense in depth approach for domain security. It started as a military strategy to protect a targeted asset, and corresponds well to domain security by providing the coordinated use of multi-layered security countermeasures.



1. **Incorporate secure domain, DNS, and digital certificate practices into your overall cyber security posture**
2. **Use a defense in depth strategy to secure your domains, DNS, and digital certificates**
   - Select an enterprise-class provider
   - Secure access to domain and DNS management systems (two factor authentication, IP validation, federated ID)
   - Control user permissions
   - Leverage advanced domain security features
3. **Proactively identify, understand, and employ the appropriate security measures for your vital domain names through CSC Security Center℠**
   - Continuous vital domain name identification
   - Registry lock
   - DNSSEC
   - DMARC
4. **Consolidate your domain, DNS, and digital certificate providers into one enterprise-class provider**

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 help them 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.

References

1. forbes.com/sites/daveywinder/2020/05/05/godaddy-confirms-data-breach-what-19-million-customers-need-to-know/