The Impact of Enterprise-Class Domain Registrar Utilization on Overall Security Ratings

SecurityScorecard.com
info@securityscorecard.com

214 West 29th St., 5th Floor
New York, NY 10001
1.800.682.1707

SecurityScorecard CSC

Executive Summary

Most cyber-attacks, including ransomware attacks and business email compromise (BEC), begin with phishing. In the early stages of a ransomware attack, phishing serves as the launch pad. Although losses due to ransomware are now in the billions[1] annually, most ransomware protection and response measures do not adequately address phishing risks.

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 email spoofing. Engaging with an enterprise-class domain registrar can help to defend against these risks.

The selection of your domain registrar is an indicator of the overall security posture of an organization.

Research done by SecurityScorecard shows that an organization's choice in domain registrar is highly correlated to its cybersecurity rating. Organizations that selected enterprise-class registrars (ECRs) for domain management versus consumer-grade domain registrars (CGRs) had a total score that was on average at least one-half to one letter grade higher.

Attributes of an Enterprise-Class Registrar

There are two types of domain registrars: consumer-grade registrars and enterprise-class registrars. Consumer-grade registrars focus on domain services, websites and email for personal use or small businesses. While CGRs are not inherently malicious, they often do not offer domain security capabilities and controls or a focus on IP protection.

Enterprise-class registrars have a mission and focus on cybersecurity and IP protection with an emphasis on domain security via advanced services and tools. Furthermore, they do not provide domain services through retail websites or pay-per-click, domain spinning, and domain auctioning services that can facilitate the infringement of intellectual property and trademarks.

Key features of an enterprise-class registrar to look for are:

- **Enterprise-wide scale and expertise** with corporate-only domain, DNS, and certificate management offering.
- **Advanced services** such as domain registry lock, DMARC, DNSSEC, CAA records, and DNS hosting redundancy.
- **Global and local 24x7x365 support capabilities** with worldwide domain registration capabilities.
- **Implementation of Know Your Customer (KYC)** methods of sourcing and validating client interactions.
- **Offer domain, brand and fraud monitoring** and enforcement and takedown capabilities.

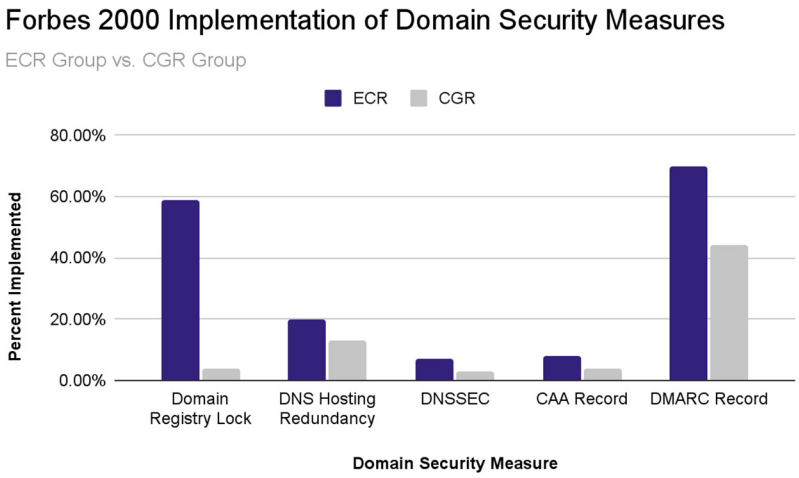
Assessing the Domain Security of the Forbes Global 2000

The 2021 CSC Domain Security Report revealed that despite the widespread shift to modernize business and operations among Global 2000 companies, web domains remain dangerously under-protected. In 2021, companies faced increased ransomware attacks, business email compromise, phishing attacks, supply chain attacks, and online brand and trademark abuse. Despite the rising cyber risk, the level of action being taken by Forbes Global 2000 companies remains unchanged.

Key findings from the report highlight the domain security risks Forbes Global 2000 companies are facing:

- **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.
- **60% of those domain registrations** have been registered in the last two years, demonstrating that this is an accelerating attack method.
- **81% of companies are at greater risk** of domain name and domain name system (DNS) hijacking because they have NOT adopted basic domain security measure like domain registry lock protocol.
- **57% of companies 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 DMARC.**

The research also reinforces these findings by comparing the implementation of domain security measures for the ECR group versus the CGR group.



Using an Enterprise-Class Domain Registrar Yields a ½ to 1 Letter Grade Increase to Overall SecurityScorecard Ratings

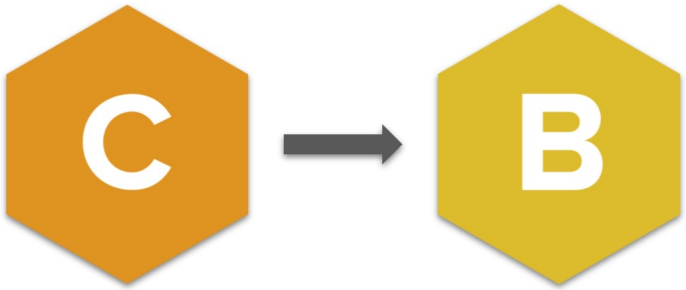
Security Ratings Highlight the Need to Prioritize Domain Security

SecurityScorecard analyzed the security ratings for 50,000 of the most followed companies in their platform and the findings continue to validate the need to prioritize domain and DNS security with a trusted enterprise-class domain registrar. Companies that selected enterprise-class registrars for domain management had a total score that was on average at least one-half letter grade higher than companies using a consumer-grade registrar. In our analysis, this made the difference between having an overall score of a “C” versus a “B.”

SecurityScorecard’s research validates that the selection of your domain name registrar is a critical decision that is often overlooked, but certainly fortifies an organization’s overall security posture.

Quantifying the Impact Enterprise-Class Domain Registrars Have on an Organization's Overall Security Rating

Out of the 50,000 organizations analyzed by SecurityScorecard, those using a consumer grade registrar had an average SecurityScorecard rating of 76.92. Organizations working with an enterprise-class domain registrar had an average SecurityScorecard rating of 81.73, resulting in a 5-point average benefit. This difference would have resulted in a full letter grade benefit from a "C" to a "B" for the ECR group versus the CGR group.



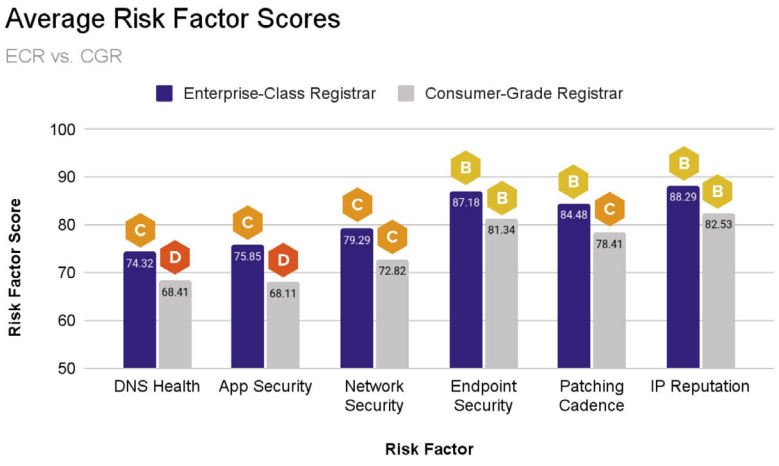
DNS Health Determined to be the Lowest Ranking Risk Factor Score Despite Being a Significant Scoring Factor

The SecurityScorecard platform measures multiple DNS configuration settings, such as OpenResolver configurations as well as the presence of recommended configurations including, DNSSEC, SPF, DKIM, and DMARC.

Despite being a significant scoring factor in Security-Scorecard's scoring algorithm, the companies analyzed had an average DNS Health score of 71.36 (Letter score of C). As a result, DNS Health was the lowest ranking factor score amongst the factor scores we analyzed. The ECR Group had an average SecurityScorecard DNS Health factor score of 74.32 versus 68.41 for the CGR Group, which was close to a 6-point average benefit difference. This would have resulted in a full letter grade benefit from a C to a D for the two groups.

DNS Health Affects Other Key Risk Factors

Our study also showed that other factor scores such as Application Security, Network Security, Endpoint Security, Patching Cadence, and IP Reputation had a 5+ point difference for the ECR group versus the CGR group, resulting in a full letter grade benefit across several factor scores.



This analysis shows that the adoption of proactive domain security measures help fortify DNS Health as well as other factor scores, thereby resulting in a higher security rating overall.

CSC & SecurityScorecard: An Alliance Based on the Fundamentals of Cyber Risk Prevention

SecurityScorecard, the global leader in security ratings, entered a strategic alliance with CSC to offer domain security insights to their clients. By taking very sensible, proactive measures to protect against domain and DNS attacks, organizations and cyber insurance providers can better pinpoint potential cyber risks, brand phishing abuse, and breaches before they occur.

While domain security requires a defense-in-depth approach of advanced security measures and operational protocols, the type of registrar you select also really matters as we see the impact supply chain has with attacks such as SolarWinds. Traditional ways of looking at DNS security were more focused on DNS resiliency, resolution, and related DDoS protection. A key component of DNS health that is overlooked today is how domains and DNS are being manipulated to conduct malicious attacks on an enterprise and their consumers.

The Three Pillars of Domain Security

CSC's focus on domain security is threefold:

1. Ensure that legitimate domains and the DNS tied to them are not being compromised at your domain registrar or DNS hosting provider (DNS hijacking, domain hijacking, subdomain hijacking).
2. Monitor and deactivate malicious third-party domains.
3. Ensure that email authentication is being used to protect against email spoofing.

CSC Domain Security Best Practices

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 domain registrar.

CSC recommends four key strategies:

1. Adopt a defense-in-depth approach for domain management.
2. Confirm that your domain registrar's business practices are not contributing to fraud and brand abuse.
3. Continuously monitor the domain and DNS space as well as key digital channels like marketplaces, apps, social media, and email for brand abuse, infringements, phishing, and fraud.
4. Leverage global enforcement, including takedowns and advanced techniques in internet blocking.

Conclusion

The continued proliferation of ransomware and security challenges resulting from remote work policies has made choosing a reputable domain name registrar a vital decision for those responsible for cybersecurity risk mitigation and online brand protection. Choosing an enterprise-class registrar that prioritizes security, data governance, and global support is critical to protecting an organization's brand and customer safety.

SecurityScorecard and CSC have partnered to educate and mitigate security risks posed by the lack of domain security measures that start with the selection of your domain name registrar.

Closing statement

Sign-up for a complimentary SecurityScorecard Enterprise License that enables you to monitor your own organization and up to five vendors here.

Sign-up for a complimentary CSC Domain Security Audit here.

[1] https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=75f066bf71c6

Resources

For a comprehensive list of best practices:

CSC 2021 Domain Security Report

CSC Blog

Five Steps to a Modern Cyber Risk Management Team

The Perfect Scorecard: Getting an A in Cybersecurity from your Board of Directors

SecurityScorecard Blog

About CSC

CSC is the trusted provider of choice for the Forbes Global 2000 and the 100 Best Global Brands® for enterprise domain names, domain name system, and digital certificate management, as well as digital brand, fraud, and phishing protection. We secure companies against cyber threats to their online assets using our proprietary security solutions, helping them avoid devastating revenue loss, brand reputation damage, or significant financial penalties.
We also provide a combination of online brand monitoring and enforcement, taking a holistic approach to digital asset protection. Learn more about our domain management, security, brand protection, and fraud protection services at cscdbs.com.

About SecurityScorecard

SecurityScorecard helps enterprises gain operational command of their security posture and the security posture of their third-parties through continuous, non-intrusive monitoring. The company's approach to security focuses on identifying vulnerabilities from an outside perspective, the same way a hacker would. SecurityScorecard's proprietary SaaS platform offers an unmatched breadth and depth of critical data points including a broad range of risk categories such as Application Security, Malware, Patching Cadence, Network Security, Hacker Chatter, Social Engineering, and Leaked Information.

To receive an email with your company's current score, please visit instant.securityscorecard.com.

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.com
@security_score

SecurityScorecard HQ
214 West 29th St., 5th Floor
New York, NY 10001