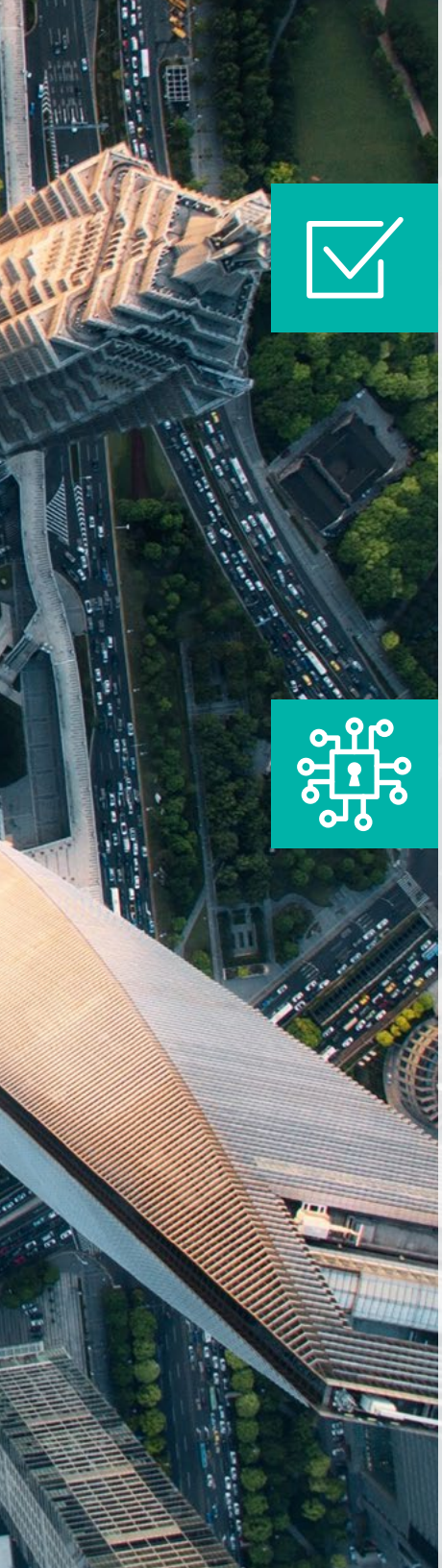

CSC
MIDMARKET BUSINESSES:
Staying Ahead of Risk for Your Future Initiatives

Maintaining a steady growth trajectory and recruiting the right talent has been a challenge for small and midsize businesses (SMBs) after a year marked by a global pandemic. Hybrid or remote work enablement and investing quickly into digital transformation initiatives has added additional burdens to these businesses.

The technology- and digital-driven world is here to stay. Midmarket businesses will need to embrace the additional burden that lay in front of them—from protecting digital intellectual property (IP) such as domain names, apps, and brand names on the market place, to properly securing their assets such as domain name system (DNS) and digital certificates as part of their cyber security risk posture. Digital IP and cyber security should be part of any organization's risk management strategy as any disruption can mean an immediate threat to an organizations' ability to operate normally.



BUILDING AND MAINTAINING A STRONG BRAND MEANS PROTECTING AND SECURING YOUR DIGITAL ASSETS

Midsized companies might own smaller portfolios of digital assets, yet with growth—within the market and potentially expanding business abroad—this will gradually change. Understanding how to protect IP online and how to manage risk is not only important, but if managed and secured correctly, can help quickly build and maintain a company's brand recognition and reputation.

Managed poorly, intellectual property issues can hold back brand expansion and sully a good reputation. Businesses today are crossing state and international borders via the internet—either willingly to offer their products and services, or unwillingly when their products are used for cybersquatting purposes or when copied and sold as counterfeits. With the abundance of digital platforms and the expanding digital landscape including new generic top-level domains, mobile apps, and more—protecting and securing your brand online becomes more challenging every day.

PROTECTING YOUR DIGITAL ASSETS

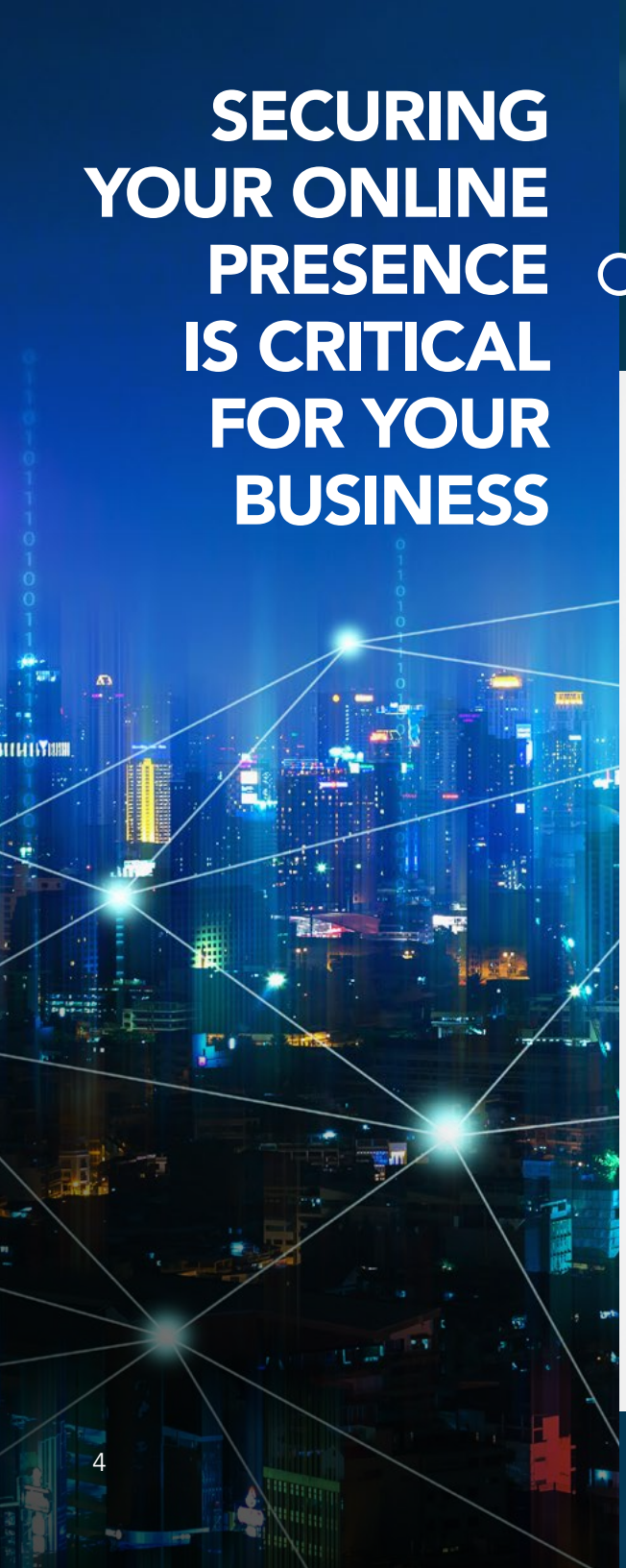
Now is the time to choose a provider that understands the business of protecting and securing your digital portfolio, and consolidating from multiple providers to one. A good provider will advise you which domain names to register now in preparation for expanding your business, and encourage you to centralize all your digital assets so you get an overview of what you own and how each domain performs.

You should be able to trust your provider to understand the challenges of registering domains anywhere you want to do business, not just your home country, but also abroad, for example, in Canada or the United Kingdom. A provider should also be able to help you set up the right Secure Sockets Layer (SSL) certificates to give your clients confidence when sharing sensitive information on your website. In addition, your provider should offer you cost-effective security services like registry and registrar locks, two-factor authentication, and multi-layer authorization, which will combat hijacking of your business-critical domains by protecting you against unauthorized changes and deletions.

Keeping an eye on your brand(s) across a growing number of global digital channels is hard. And with the complexity of online threats increasing, online reputation monitoring is becoming more complex. Speak with your provider to review your brand(s) as well as your digital assets. A simple audit should determine which monitoring solutions you really need. There is no one-size-fits-all approach when it comes to monitoring your brands online.

The industry you're in and the channels you use to communicate and sell to your customers will determine what you really need.

SECURING YOUR ONLINE PRESENCE IS CRITICAL FOR YOUR BUSINESS



DOMAIN NAMES

Domains are the core element to the digital landscape of a business—powering corporate websites, email, virtual private networks (VPN), and other corporate applications. When those domains are compromised, criminals can redirect websites for financial gain, intercept email to conduct espionage, and even harvest credentials to breach networks. This will have a significant impact on a company's revenue and reputation.

In short, domain names are foundational components to a company's ability to operate in this day and age. CSC recommends using the principles of a defense in depth strategy for domain security, with the coordinated use of multi-layered security counter measures, including:

- Enterprise-class provider
- Secure portal access
- User permissions control
- Advanced security features for business-critical domains

DOWNLOAD THE FULL CHECKLIST HERE. →

DNS

DNS connects everything to the internet—laptops, tablets, mobile phones, websites, and any other smart devices—and relies on accurately associating domain names with their corresponding IP address.

Reliable DNS service is crucial to doing business well. Without it, your websites and online applications are vulnerable to outages, attacks, and email disruptions. The long-term risks of inferior DNS service include customer frustration and negative brand associations.

Whether you're fully outsourcing your DNS or partnering with a provider to supplement your own DNS infrastructure, the business-critical nature of DNS means it is one of the most important decisions you will make as an organization. Consider the following:

- How much downtime can my business afford?
- How long would a distributed denial of service (DDoS) attack take to resolve, and what would it cost my company?
- Do I have multi-layered security measures and countermeasures in place to defend my businesses against malicious attacks like DDoS, DNS hijacking, and DNS cache poisoning?

BRAND PROTECTION

Keeping watch over your brands across all digital channels is a continuous challenge. Online threats are constantly evolving, making it challenging to monitor potential online brand infringements. Developing a strategic brand protection and monitoring strategy is crucial to maintaining your brand's integrity and rights.

- What kind of brand protection does your company really need?
  - » Internet monitoring
  - » Domain monitoring
  - » Social media monitoring
  - » Mobile app monitoring
  - » Paid search monitoring
  - » Marketplace monitoring
- Does my company worry about counterfeits?
- What type of enforcement actions are available?

The digital world is evolving and no less dangerous than it was before the global pandemic. SMBs may need help embracing the additional burden of protecting and properly securing digital assets to continue operating normally.

PHISHING

The number of phishing attacks observed by the Anti-Phishing Working Group (APWG) and its contributing members doubled during 2020. This trend, considering the shift to the digital world, will most likely remain for the unforeseen future. Phishing emails, electronic messages, and websites remain all-too-common vehicles for corporate data breaches, credit card fraud, and identity theft when phishing emails are taken seriously, links are clicked, or private information is exchanged.

To prevent this situation from happening to your company and clients, work with a provider to tailor a solution that fits your security needs and reporting requirements.

DIGITAL CERTIFICATES

Digital certificates, like SSLs, are the fundamental building blocks to success for your online business, as they provide authentication for websites and enable an encrypted connection for you and your customers. If not maintained or replaced before expiration, the lack of up-to-date digital certificates creates vulnerabilities that cyber criminals can take advantage of. Unlike other digital services that renew automatically, SSL certificates expire, leading to inevitable risk. Think about how you:

- Account for all existing certificates
- Cross-reference SSLs with live sites
- The policy and process for correct SSL management
- Regularly audit SSLs (including contacts in the system for SSL renewals)

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 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.

cscdbs.com

DBS10192021