CSC

Digital Asset Security:

Back to Basics

Digital Asset Security: *Back to Basics*

The many cyber attacks and data breaches worldwide show that these incidents are becoming more intense, are on the rise, and the environment has become much more complex to secure. While businesses continue to invest in technology, those working to secure organizations are challenged every day.

Many of the current security methods, tools, and techniques used by businesses to secure their environment and protect their brand have been effective so far, but attacks are now coming from all directions. Hackers, hacktivists, cyber criminals, nation states, and insiders (like employees) are all pounding security protocols to find a weak spot to get in.

Knowing that data streams in from various entry points, organizations that still differentiate between internal and perimeter security should urgently reconsider their security approach—specifically the roll of digital assets (i.e., domains, domain name system (DNS), and digital certificates)—in enabling the day-to-day successful operation of their business.

How can you shift from a traditional cyber security approach to an approach that will mitigate today's risks?

Understand and identify your digital assets to manage them properly.

Grasp the implications of an incident to your business and plan accordingly.

Optimize your ROI. You need to know what's valuable (think vital domains) and what is not.

Defend the many digital channels.

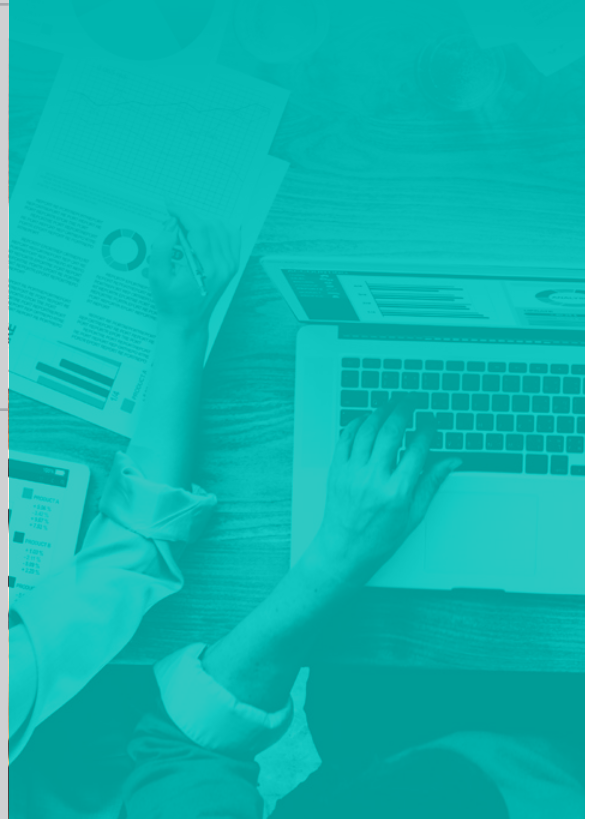
1

2

3

4

Understand and identify your digital assets to manage them properly.



Over the past 20 years, your organization has accumulated a large number of digital assets. Those digital assets represent your company, enable your organization to conduct transactions, and ensure smooth communication and interaction with clients, vendors, and colleagues. In short, those assets have changed the way you communicate, operate, and consume.

Today, the world is more connected than ever before—and while this is a fantastic opportunity for businesses around the world, it also has its challenges. As the global digital economy develops, so do online assets, like domain names, digital certificates, social media usernames, and mobile apps. So it's imperative for companies to understand what online assets they own and use. Failing to do so will make a business vulnerable to brand infringement and cyber attacks.

It's likely that the complete information of what's owned and what's actually used is scattered between various departments—including marketing, legal, IT, and sometimes even human resources—so the best way to start is to create a list of all online assets, asking your providers and registrars to conduct an audit. Every company should look at this holistically—meaning, while you might work in the U.S. office, look at online assets globally in all the regions where your company operates.

Here's a checklist. Determine:

- ○ **The domain names you own, including those registered for promotional purposes (like vanity URLs) and defensive reasons**
- ○ **Who provides your DNS for each domain, whether it's your domain registrar, a specialist DNS provider, or an infrastructure you support yourselves**
- ○ **The number of digital certificates you have, including the validation type of each, and how they are being managed**
- ○ **The number of social media handles you have across platforms**
- ○ **Who has access to the social media usernames and passwords, and how the handles are being managed**
- ○ **If you've created and published mobile apps, and how they're being managed**

Importantly, when compiling this information, it's essential to also understand who has access and to what.

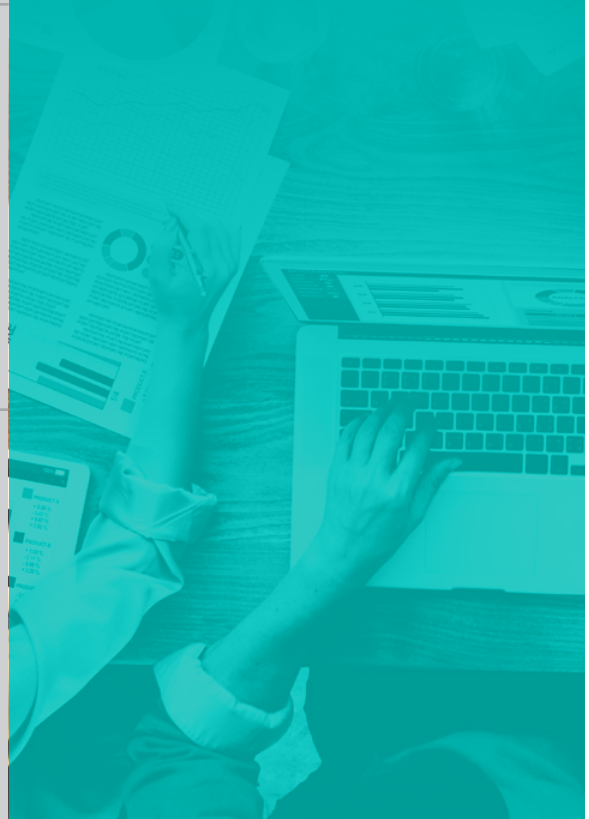
1

Understand and identify your digital assets to manage them properly.

2

3

4



Consolidate your online assets with enterprise-class providers

Understanding your global organization's needs as it pertains to domains, DNS, and digital certificates will ensure that each provider you work with meets the criteria that you require. For each area, there are a wide range of providers from low cost "do it yourself" providers with limited service models and billing models relying on credit cards, to enterprise class, providing "white glove" service, as well as the SLA, liability, and billing models you require as a global company. Your chosen partners' security posture should also be a major consideration.

In addition to looking carefully at the quality of your providers, a suggested best practice is to consolidate your online assets to ensure smooth management and business continuity. Being able to manage all your online assets through one dedicated team and, ideally, one platform, will make you more adaptable to changes, including registering or lapsing domain names, changing social media credentials, renewing digital certificates, and more. Most importantly, it will give you a clear overview of your security weaknesses.

Ask prospective or current providers to conduct an audit of your online assets. If you're not already, work with an enterprise-class provider. They're the most likely to offer the best possible digital certificates, domain, and DNS management. They should also be able to monitor all domains under their management to enforce your consolidated DNS and digital certificate policies. Some questions you'll want answered include: which domain names aren't live or are not resolving properly? Which business-critical domain names aren't using domain name system security extensions (DNSSEC)? And is "SSL Always On" enabled on your business-critical domains?

At a minimum, this type of audit should be regularly scheduled maintenance to regulate your policy and identify domains registered outside of the policy. With the very best provider, the analysis will be as close to real-time as possible, with notifications to alert you to potential issues or non-compliance. That means, you also need to educate staff once you've established a policy you expect them to follow.

Learn more in point 4.

1

2

3

4

Grasp the implications of an incident to your business and plan accordingly.

This enables you to revisit what happens if there's an issue, and tie it back to business continuity, making it a boardroom discussion—which is key.

The 2018 Business Continuity Institute's annual **BCI Horizon Scan Report** identifies the top 10 business continuity risks, as reported by 657 respondents in 76 countries. And perhaps surprisingly to some, digital assets play a contributing factor in four of these risks:

- **Cyber attacks.** The DNS is vulnerable to a whole host of cyber attacks ranging from DNS cache poisoning, DNS hijacking, domain shadowing, malware, DNS tunneling, distributed denial of service (DDoS) and phishing attacks, as well as the exploitation of expired digital certificates.
- **Data breaches.** Cyber attacks against digital assets are increasingly used to steal data, either by masking another attack vector or by directly taking advantage of poor security and management of assets.
- **Unplanned IT and telecom outages.** If a company's domains or DNS fail, then every way it communicates using the internet can fail. If that happens, how would an organization communicate with clients and employees?
- **Supply chain disruption.** Since a failure of company domains and DNS will grind to a halt the ability to communicate, how would a business maintain operations and supply chain?

It's clear that the implications are high and applying basic security measures to your online assets is vital. The severity of cyber attacks is increasing around the globe, so it doesn't really matter if you're being attacked by hacktivists or cyber criminals—the fact is that when it happens, it will cost the company dearly.

Ask yourself

- Have you secured access and permissions to all your digital assets?
- What DDoS protection is your company using?
- What phishing or email fraud solution is your company applying?
- Does your DNS provider give you a 100% uptime guarantee?
- Do they have a credible history of providing this guarantee to their clients?
- Have you applied all available additional security features to your business-critical domains, appropriate for your business and the level of risk you face?

1

2

3

4

Grasp the implications of an incident to your business and plan accordingly.

Understand which assets are business critical

An essential consideration is understanding which of your digital assets are business critical. This sounds like it's easy to do, but in reality, you need to understand how domains are being used by different functions across your business globally.

Our recommendation is to partner with a provider who has built an algorithm or is moving towards machine learning that can identify your business-critical domains as vital assets in as close to real time as possible.

Employ a defense in depth approach

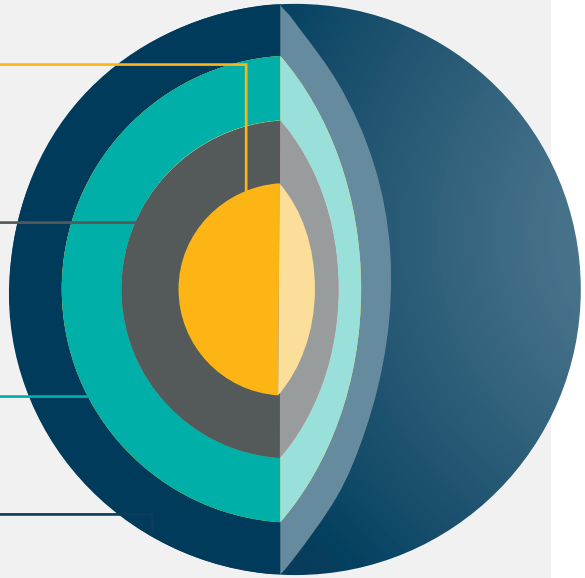
Defense in depth is the concept of a multi-layered security approach, defending your digital assets against the many threats that can lead to the aforementioned business continuity risks.

EMPLOY ADVANCED SECURITY FEATURES FOR BUSINESS-CRITICAL DOMAINS
MultiLock, DNSSEC, HTTPS, DMARC, and CAA Records

CONTROL USER PERMISSIONS
Visibility on elevated permissions and notifications

SECURE PORTAL ACCESS
IP validation, two-factor authentication, and federated ID

ENTERPRISE CLASS PROVIDER
Systems, staff, policies, and processes



1

2

3

4

Optimize your ROI. You need to know what's valuable (think *vital domains*) and what is not.

First, the nature of digital assets—and domains in particular—being relatively cheap to obtain, has resulted in bloated portfolios with poor ROI. But it's possible to prove ROI, and this is especially important given that businesses are finding it necessary to spend more on advanced security features for vital domains. The concept is simple, lapse and divest assets that are not valuable to your brand to help fund the additional security investment required.

You'll want to ensure your digital IP resolves to relevant content. Then you can measure traffic —a key indicator of ROI. You could still be holding on to domains from special campaigns that are no longer active or have been redirected to a main domain. You may also want to review domains that have been registered for defensive purposes. While they might not garner much traffic, they may defend your trademark against infringement. Keep the defensive registrations if they're necessary, and where possible, safely divest unnecessary domains to optimize your portfolio. This gives you room to identify gaps related to available domains, including brands, and register those if need be.

However, an abandoned corporate domain name often carries a footprint of activity that can be leveraged as an attack vector. Therefore, any rationalization or divestiture exercise should be carefully undertaken with an enterprise-class provider. Those that have the tools to identify vital domains will be best to ensure that you only rationalize or divest those domains of no true value to you.

1

2

3

4

Defend the many digital channels.

Once you have control of your own digital assets, it's time to look at the assets owned by third parties who are leveraging your brand or perhaps pretending to be you.

Online monitoring services are an important asset in most industries. The degree to which you use monitoring depends on your own digital brand strategy, and you should again engage with legal and marketing at your company to help determine what's important to monitor closely and what you don't have to worry about.

Consider that while you want to mitigate security risks, legal and marketing want to prevent your brand from being infringed upon. Despite different motives, your common goal is the same—safeguard your company!

When your digital brand monitoring activities are based on your priorities, they're more cost-effective and more likely to spot the most damaging threats. You'll be able to identify the bad guys before they get anywhere near your valuable property. Once you have the right monitoring solution for your brand in place, you can determine which alerts are most critical to address immediately and possibly ignore the ones that won't affect your brand. But know that filtering the monitoring results will become a constant job.

Monitoring will also enable you to police your security policies and controls. That starts with ensuring that all staff register domains through your centralized, chosen domain management partner. Then it's important to look at the associated DNS and digital certificates, determining whether the domain is vital, and if all the proper security features have been employed based on the domain's importance to your brand.

A good brand monitoring provider can help you manage the constant barrage; an excellent provider will even sift through the alerts for you, providing you with only the most critical infringements that need your attention.

CSC Security Center

CSC Security Center℠ meets a previously unfulfilled industry need—complete security oversight of your business critical domains. This one-of-a-kind solution was created using CSC's advanced proprietary algorithms to be the most comprehensive domain security solution on the market. It will identify vital domains, monitor for ongoing threat, send notifications when changes occur, and make threat mitigation simple. We encourage you to learn more about CSC Security Center and how it can transform the way you manage digital assets while mitigating cyber risks.

cscdigitalbrand.services

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