CSC

digital asset SECURITY CHECKLIST

DIGITAL ASSET *vendor management*

- □ You have a FULL accounting of all your domains, domain name systems (DNS), and secure sockets layer (SSL) providers.
- □ All your digital asset providers deliver enterprise-level support 24/7/365.
- □ All your digital asset providers have invested heavily in protecting their systems, e.g., ISO 27001 accredited data centers, SOC 2® compliant, third-party penetration, vulnerability testing, and security tests, including SQL injection and XSS, etc.
- □ All your digital asset providers have invested heavily in training their staff, e.g., security training, phishing awareness, including regular phishing email testing, two-factor authentication for outside network (remote) access, etc.
- □ All your digital asset providers have invested heavily in protecting their customers, e.g., IP validation, two-factor authentication, authorized contact policy, always in writing and never via phone (orders/requests), and federated identity, etc.
- □ None of your providers have a track record of succumbing to phishing, social engineering, DNS hijacking, or distributed denial of service (DDoS) attacks.
- □ All your digital asset providers primarily utilize their own accreditations rather than solely replying on third parties, e.g., your domain provider primarily utilizes their own accreditations directly with the registries and your certificate provider is an accredited Certificate Authority in their own right.

DOMAIN *management*

- □ You have a FULL accounting of your entire domain name portfolio.
- □ You have an auto-renewal policy in place with your providers that is supported by credit on account.
- □ All staff members are trained in, and adhering to, a centralized process for registering new domains.
- □ There are clear guidelines on the WHOIS template and user defined fields that must be provided at point of registration.
- □ You follow a procedure to identify company registrations that fall outside the centralized policy.

DNS *management*

- □ You have a FULL accounting of your entire DNS provider portfolio.
- □ You follow a procedure to identify domains not on enterprise-level DNS with a credible 100% uptime guarantee.
- □ All staff members are trained in, and adhering to, placing all new vital domains on enterprise-level DNS.

SSL *management*

- □ You have a FULL accounting of your SSL providers.
- □ All staff members are trained in, and adhering to, a centralized process for purchasing new and replacing old certificates.
- □ You follow a procedure to identify any SSL certificates purchased outside of your centralized policy.

VITAL (BUSINESS-CRITICAL) DOMAIN *management*

- □ You can immediately identify all vital domains and demonstrate they are secure.
- □ All DNS providers for your vital domains have a credible, 100% uptime guarantee and corresponding track record.
- □ All vital domains use a suitable enterprise-level SSL certificate.
- □ All vital domains are utilizing domain name system security extensions to protect against DNS cache poisoning.
- □ All vital domains are employing MultiLock to protect against DNS hijacking.
- □ All vital domains are employing email authentication services.

THREAT MITIGATION *continued*

- □ You use additional DDoS mitigation services to protect other servers beyond DNS.
- □ You use email authentication services combined with phishing monitoring and takedown services to minimize the threat from phishing attacks.

☎ 1 800 927 9800 cscdigitalbrand.services