CSC

CSC Security Center
Quick Guide

With cyber attacks already a daily occurrence and increasing, it's more important than ever that those charged with defending a brand's online presence choose the right partners and tools for the job.

Digital assets are known to be a weakness exploited by cyber criminals and hackers, and so it's no longer enough to choose basic management services and simply review your approach annually.

To stay ahead of cyber criminals and to assist brand owners with their rapidly evolving business models, CSC developed the CSC Security Center^{SM}, which removes the complexity and puts control back in the hands of our clients.

What are the risks and how does CSC Security Center help me?

Using multiple data sources and a complex algorithm, tested on some of the world's largest organizations, CSC Security Center is able to identify and monitor your business-critical digital assets, providing an ongoing risk assessment. This allows you to instantly recognize and mitigate the potential threats of a cyber attack against the monitored assets.

Risks	Consequences	Impact	CSC solution
Poor accounting and management	Expiration of vital domains and secure sockets layer (SSL) digital certificates	No website resolution, email, virtual private network (VPN), or voice-over IP (VoIP); loss of consumer confidence, and possibly vulnerable to a malware or ransomware attack	Audit and consolidate domains, domain name system (DNS), and SSL
Third-party providers	Social engineering, phishing, or distributed denial of service (DDoS) attack	No control over website resolution, email, VPN, or VoIP—and potential that cyber criminals clone sites and steal email	Focus on security; we invest heavily in technology and staff
Accessibility of assets	Social engineering, phishing attack	No control over website resolution, email, VPN, or VoIP—and potential that cyber criminals clone sites and steal email	Secure access to management system using IP validation, two-factor authentication, and federated identity
Third-party threats	Failure to mitigate DDoS and phishing attacks	No website resolution, email, VPN, or VoIP—and acts as a smoke screen for a second attack	Secure assets from the known threats using MultiLock, DDoS mitigation, email authentication, and anti-phishing services
A static approach	Vital domains and risks not identified	No control over website resolution, email, VPN, or VoIP—and potential that cyber criminals clone sites and steal email	CSC Security Center