WHY COMPANIES WILL NEED BETTER INTELLIGENCE AND SECURITY TO PROSPER IN 2021

As the world continues to grapple with the effects of COVID-19, we predict that companies will continue to find ways to adjust to the situation they are faced with—to explore new channels of revenue, connect with their employees and customers, and address a growing need to tighten on cyber security and online brand protection.

DIGITAL TRANSFORMATION AND ADVANCEMENTS FOR STRONGER ONLINE PRESENCE

A McKinsey & Company survey found that the pandemic accelerated digital transformation in APAC businesses by more than 10 years. Businesses that reported declining revenues are placing greater emphasis on digital. Consumers have increased their adoption of using digital channels to interact with organizations, through e-banking, online grocery shopping, and even placing contactless dining orders through e-menus at restaurants on their mobile phones.

This increased reliance on digital transactions will bring with it an increased risk from cyber criminals for both consumers and companies – through hacking, counterfeiting, and online fraud. CSC research shows an exponential increase in domain name registrations in 2020, and not all of these are registered legitimately by the businesses concerned. The Anti-Phishing Working Group's latest quarterly report shows the number of unique phishing websites detected and brands targeted by phishing campaigns are at its highest in 10 years. Around 80% of the phishing sites use digital certificates to give a false sense of security to unsuspecting web users, clearly indicating that cyber criminals are upping their game and phishing activity.

In 2021, we expect to see continued advancements in digital enablement, and businesses developing innovative online strategies. At the same time, organizations will need to protect against infringing sites and content to strengthen their online presence, and prevent brand dilution from traffic diversion, customer confusion, phishing attacks, malware distribution, and the sale of counterfeit goods.

MAINTAINING CONNECTEDNESS IN A SAFE-DISTANCED WORLD

In 2020, IT professionals were challenged to deploy work-from-home environments with little notice, having to provide employees with VPN access and many cloud-based solutions when COVID-19 struck. Being online and maintaining operational uptime for employees and customers has never been more important.

Recent cyber attacks show that cyber criminals can and will find blind spots to exploit in companies' security postures, finding the weak link among third-party vendors or employees to infiltrate company networks through ransomware or social engineering, or crippling them with DDoS attacks.

Three-quarters of surveyed cyber security professionals anticipate increases in DNS attacks that could take down their organization's online presence and damage their brand reputation, but 30% have reservations about their ability to respond to these attacks.

In response to the rise in sophistication and number of cyber attacks, the maximum term for certificate validity was shortened to one year in September 2020. We foresee that digital certificates' validity terms will shorten again, as the browser community in the CA/Browser Forum are pushing for 90-day term. This adds pressure on teams to ensure proper inventory of their digital certificate portfolio. Failure to replace an expired digital certificate on business-critical domains will lead to the loss of critical services for customers and employees. Furthermore, an outage can weaken a company's defenses against a cyber attack and putting customers' personal data at risk of compromise. Companies need to prepare for this impending change now.

As companies continue to embrace third-party SaaS and cloud technology for the rapid global deployment of applications and solutions, 2021 will be a time to consolidate these efforts and tighten cyber security controls, even as we see a portion of the workforce returning to offices.

INNOVATION AND BETTER INTELLIGENCE TO PROTECT BRAND REVENUE AND REPUTATION

In December 2020, the EU's General Data Protection Regulation (GDPR) took its first cross-border action since its inception in 2018, issuing a €450,000 fine to a large US tech company. Regardless of geography, companies are held accountable for data breaches under GDPR. This same regulation, however, has made domain registries redact WHOIS information, making it more difficult to identify and take enforcement action against cyber criminals abusing a brand. Companies cannot relax their defenses against data breaches, and have to go on the offensive, finding effective means to investigate and enforce on the threat actors infringing their privacy or intellectual property rights.

As we hope for a brighter 2021, we recognize the challenges that come with it. CSC advocates a Defense-in-Depth approach to protect our clients' brand reputation and revenue:

- **Enterprise-class:** We are an ICANN- and registry-accredited enterprise-class provider that invests in our systems and security; including both staff training on cyber security, as well as a variety of processes and security controls.
- **Secure portal access:** Our portal access is secured with two-factor authentication, IP validation and federated identity for a single sign-on environment.
- **Control user permissions:** We enforce an authorized contact policy, alerting clients when there are changes in permissions, especially those with elevated permissions.
- **Leverage advanced domain security features:** Our proprietary, predictive modeling algorithm, identifies domain names that conduct business-critical work for our clients' business operations and online brand, and we recommend security controls such as DNSSEC, registry locks, and DMARC on these vital domain names.

- **Proactive, continuous monitoring and alerting:** We monitor for unauthorized changes to your domains, DNS and digital certificates, as well as unauthorized use of brands within third-party-registered domains and websites, social media, marketplaces, mobile apps and more.

Through our domain name portfolio management, online brand and fraud protection, as well as domain security defense, we provide comprehensive 360 cyber security coverage towards detecting and mitigating cyber threats targeting businesses, and continue to enhance our platforms with innovative engines that are able to provide better intelligence for our clients to secure and protect their online brand presence. As the trusted and most security-conscious provider of choice for the largest global companies, we are committed to helping our clients mitigate threats and minimize risks, to ensure uninterrupted business continuity, brand performance, and secured revenue amid these challenging times. ACO

APAC CIOoutlook is a print magazine that reaches out to 60,000 qualified subscribers across the Asia Pacific region and 1,80,000 digital subscribers across the globe that aims to provide a platform for CIOs, CTOs and other senior levels technology buyers and decision-makers along with CXOs of solution providers to share their experiences, wisdom, and advice with Enterprise Tech community of APAC countries. We promote our unique 'learn from our peer's approach' in the Asia Pacific region.