



# **DOMAIN SECURITY**

## **A Critical Component of Enterprise Risk Management**

**Prepared by  
Dave Piscitello, Dr. Colin Strutt, and Lyman Chapin  
Interisle Consulting Group, LLC**

**28 June 2021**



## Executive Summary

New, evolving, or persistent threats - ransomware, Business Email Compromise, information stealing, and targeted phishing attacks – appear almost daily. Email, counterfeit, or malicious web content are common indicators among such attacks, and they cause financial losses or disruptions to critical services or infrastructures that threaten lives or lifestyles.

Perpetrators of these attacks victimize users through some form of deception; for example, they use domain names or hyperlinks that “look like” high value brands or organizations they have targeted. They also use persuasion (social engineering) to compromise or hijack domain names that can lend temporary legitimacy to their attacks. Cyber-attack perpetrators commonly acquire domain names from registrars that focus on volume and whose business practices in a domain registration marketplace make look-alike domain names easy and cheap to acquire in bulk. The commodity nature of this marketplace leaves little margin or incentive for registrars to implement measures to protect their customer accounts against attack. The combined effect of these factors streamlines the “weaponization” of domain names for criminal or malicious use and exposes risks to enterprises that typically are not addressed proactively.

In this report, we consider *domain security*, which we define as the preventive measures that reduce the risk of harms or losses associated with an organization’s domain name portfolio. We explain the threat landscape and the risks these threats pose. We describe incidents in which failing to adopt domain security measures has been the cause of disruption of service, reputational harm, or other losses. We propose what should not be, but apparently *is*, a novel strategy: include domain names in your enterprise risk management. We then explain how to navigate your way to a registrar that can serve as an enterprise risk management partner.