****

**Cyber Security – Elite Services**



.

**Cyber Threats and Strategy**

Cyber threats and attacks continue to grow in number and complexity—all while the business world grows increasingly connected and digital. As every aspect of business today touches on some digital component, cyber risk concerns stretch well beyond IT and well beyond the walls of the enterprise—to every partner, vendor, customer, worker, and to every business process.

Amid this new landscape, managing cyberthreats becomes a business and strategic imperative. Tangible costs from cybercrime range from stolen funds and damaged systems to regulatory fines, legal damages, and financial compensation for affected parties. Intangible costs could include loss of competitive advantage due to stolen intellectual property, loss of customer or business partner trust, and overall damage to an organization’s reputation and brand.

With so much at-stake, business today should treat cyber threats us a top-tier business risk, requiring a comprehensive strategy which entails tailor made solutions and controls unique to the particular business needs and goals.

This document outlines our proposed approach to enhance cyber readiness and defense, to minimize critical risk and to demonstrate the company responsibility through a comprehensive approach at the highest standard in accordance with regulatory requirements

**Our Elite Solutions**

**Simulations &war-gaming methodologies** used to help decision-makers, top executives and professional senior leadership to effectively discharge their responsibilities for protecting critical infrastructure, assets and procedures that are essential to the normal functioning of modern society. This helps clients to examine cyber issues through the application of the principals of Systems Thinking, to address dynamic problems that require constant learning and adaptation.

 Our methodologies may respond to various needs across the organisation. Using a military analogy, one would describe it as methodologies for tactical level, the operational level up to the strategic level. In the civilian context of the Bank, this would apply to the lower levels of management and upwards to the Bank’s most senior executive.

 

**360 degrees Red Team** a full-scope, multi-layered attack simulation designed to measure how well your people, networks, applications and physical security controls can withstand an attack from a real-life adversary.

Whenever we discuss Information Security from a defensive point of view, we are inclined to think about protection, damage control, and reaction. However, adopting an attacker’s mindset can effectively help businesses enhance their chances of securing themselves against ever-changing threats.

 Our Red Teamsare composed of people with different disciplines and specialties, and the spectrum of attack is not confined to the technological side. In this way, we more realistically simulating the ways in which a sophisticated cybercrime group operates.

Relying on those expertise to explore any possible way to plan and carry out an attack the Red Team are trying to espouse the standpoint, the attitude of potential assailants.such simulations aimed at both reproducing a real emergency and improving the ability to fend off an aggression, thus the Red Team is supposed to both identify any vulnerability in the PPT (People, Process and Technology) defensive system and help the organization improve its own defensive abilities.

****

**Who Are We**

C*stratgey* Is a boutique company engaged in providing multi-dimensional holistic solutions tailored to the customer needs.

Our team of leading experts in Risk Assessment and Cyber Security, is assembled from veterans of elite IDF &ISA operational and technical units.

Among our customers, tier-1 companies including banks, investment houses and high-tech companies. So far, we are active in the USA, Europe, Australia and Israel India.