





HOLISTIC**CYBER**



HolistiCyber's Cybersecurity Risk Assessment delivers laser-focused recommendations to improve security pragmatically and cost effectively by leveraging a holistic approach coupled with nation-state level and private sector expertise

In recent years, there has been a quantum leap in the development of tactics, techniques and procedures of powerful cyber-attack weapons. In the past, only nation-states have possessed these weapons. Today, these powerful weapons are available to various groups such as cyber terror, hacker groups, plain hackers, cyber-crime criminals and Hacktivists. Thus, these sophisticated potential cyber-attacks have become a major concern for commercial entities-not just nation-states. For cyber attackers, an intensive well-developed infrastructure of collaboration within the "Darknet", allows them to share knowledge and cyber-attack instruments easily and anonymously. This "Darknet" has led to a rapid growth of cyber breach incidents whose threats are very real, evolve and occur practically every day in growing numbers.

The first step in any defense plan is to confront cyber threats and mitigate these cyber risks by performing periodic Cybersecurity Risk Assessments.

HolistiCyber's unique holistic approach uncovers critical vulnerabilities by combining standard best practices along with assessments and diagnostics of human factors, cyber technologies and organizational processes. In addition, we leverage our broad and deep knowledge of attacker's techniques and attack technologies to deliver a Holistic Cybersecurity Risk Assessment from an attacker's perspective. This approach helps you better identify potential vulnerabilities that allow you to implement highly focused data breach prevention practices for an effective and practical defense of your sensitive information.

HolistiCyber's Cybersecurity Risk Assessment can be an organization's cornerstone to a holistic defense plan that identifies, protects, detects, responds and provides recovery from dangerous nation-state level cyber-attacks.

Our certified experts have served in the front line of nation-state cybersecurity events. They are Cyber Security Holistic analysts – people who understand your internal IT staff; can extend their bandwidth; and can perform cyber security activities your busy IT staff does not have the resources or time to perform.

Holistic Security is an approach that seeks to integrate all the elements designed to safeguard an organization, considering them as a complex interconnected system. The ultimate purpose of holistic security is continuous protection across all attack surfaces: the totality of all physical, software, network and human exposure.

Source: TechTarget

HolistiCyber's Cybersecurity Risk Assessment will Clearly Outline Potential Vulnerabilities and an Effective Mitigation Plan

HolistiCyber provides state-of-the-art methodologies; world-class, multi-disciplinary cyber security expert teams with real-life, hands-on, practical know-how; and, proven success in performing holistic cybersecurity risk assessments to both private and public sectors. We employ innovative techniques, best practices and the best of class commercial products along with our own proprietary technologies.

HOLISTICCYBER'S

Cybersecurity Risk Assessment Objectives

- ◉ Identify your Cyber Threats (threat actors, threat agents).
- ◉ Analyze your Cyber-attack-surface:
 - ◉ Technology (infrastructure, systems, and applications).
 - ◉ People (employees, outsourcing, vendors, third party providers, clients).
 - ◉ Organizational processes (business processes, lines of production, exogenous processes and supply chain).
- ◉ Map and attribute your Cyber Threat attack vectors (vulnerabilities and attack tactics, techniques and procedures).
- ◉ Identify and assess your cyber security risks driven from your Threat Map.
- ◉ Prioritize initial recommendations of how to mitigate the identified cyber risks based on your company's specific goals, schedule and budget.

Cyber Kill Chain	Protect-Prevent	Detect	Response	Recover
Reconnaissance	⊙	⊙	⊙	⊙
Weaponize	⊙	⊙	⊙	⊙
Deliver the weapon	⊙	⊙	⊙	⊙
Install, spread and hide	⊙	⊙	⊙	⊙
Establish a command and control channel	⊙	⊙	⊙	⊙
Accomplish attack, Wipe: trace / non repudiation	⊙	⊙	⊙	⊙

Legend

- ⊙ Minimal Control
- ⊙ Full/Partial Control
- ⊙ No Controls

Defense map: Summarizes the ability to address the different stages of the cyber kill chain.

Holistic Cybersecurity Risk Assessments is Tailored to Your Organization's Unique Needs

HolistiCyber understands that the keys to successful cybersecurity risk assessments and data breach prevention is the establishment and enforcement of an appropriate security level for your organization. We offer a full range of services and risk assessments to evaluate your systems, applications and processes for a variety of vulnerabilities. These include:

HOLISTICCYBER'S Cybersecurity Risk Assessments

- ◉ Mapping your organizational roles and responsibilities.
- ◉ Reviewing your key security documentations and policies in the context of protecting against cyber threats.
- ◉ Reviewing your organizational procedures in the event of a cyber-attack.
- ◉ Mapping Information Security Processes.
- ◉ Analyzing relevant constraints such as regulations, structural and operational processes, costs and efficiencies.
- ◉ Testing the integrity of your organization's core applications and their effectiveness at preventing cyber-attacks.
- ◉ Assessing the effectiveness of your organization's physical security in relation to sensitive IT systems and potential cyber security risks.
- ◉ Providing network security, mobile security and cloud security assessments.
- ◉ Performing White, Gray and Black box penetration testing, vulnerability and wireless assessments.

HolistiCyber conducts the Holistic Cybersecurity Risk Assessment as a joint project with your IT department, business stakeholders and IT security staff using a state of the art Work Breakdown Structure (WBS)

HolistiCyber's Comprehensive Set of Deliverables

The deliverables of an engagement is an extensive document detailing the relevant potential risks, which include the various breaches and attack scenarios described by articulating the probabilities of their exploitation and their possible damage to your organization's secure information. The findings are summarized in a Risk Heat Map to assist you in the decision making of an appropriate defense plan. The summary assessment report has the following topics:

HOLISTICCYBER'S Comprehensive Set of Deliverables

- Project Objectives.
- List of inspected systems and the scope of the analysis.
- Executive summary - Emphasizing the business impact of the identified highest risks and crucial threats.
- A description of our methodology.
- Cyber threat map – identification and definition of threat actors: external threats, internal threats, trusted internal threats.
- Social Engineering Findings.
- Social engineering findings - Outline report of social engineering scenarios in terms of potential compromised business processes.
- Cyber Risks - All the vulnerabilities, flaws, weaknesses and potential breaches discovered, sorted by the significance of risk and business impact.
- Summary and Recommendation - Our findings in a clear and prioritized list of recommendations and actionable initiatives for your business.

1. Level of Absolute Inherent Risk without controls

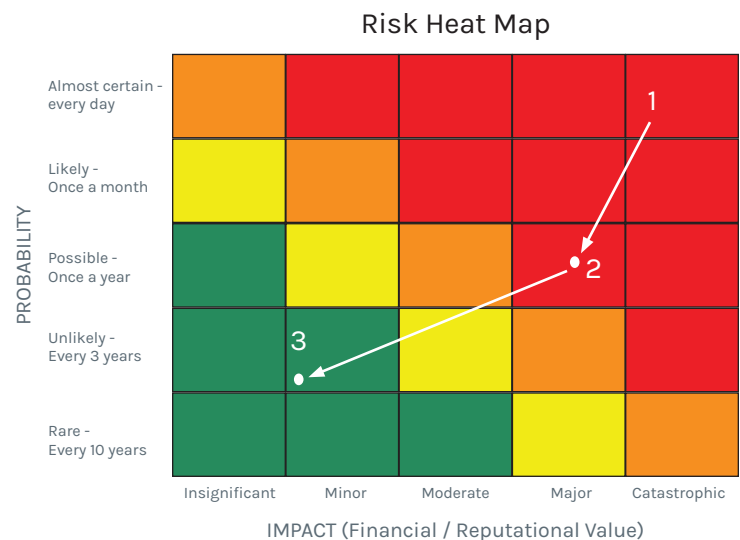
- Identify all possible risks and risk areas that are of concern and / or need attention which relate to the activity being analyzed.

2. Level of Managed Risk (with existing control)

- Identify all relevant countermeasures that do exist
- Assess the level of the prioritized risks as identified

3. Level of Residual Risk (after implementing new controls)

- Assess the level of residual risks as identified



Best Practice Gap Matrix: Indicates the current state and recommended next steps



About HolistiCyber

HolistiCyber brings a long history of experience in both the public and private sectors. Our certified analysts are cyber security veterans of the intelligence branch of the Israel IDF. They are world-class experts with a long history of public and private sector experience who have served at the front-line of critical nation-state cybersecurity offensive and defensive incidents. Our team of cyber security holistic analysts are people who understand your internal IT staff; can extend their bandwidth; and can perform sophisticated, advanced nation-state level cyber security testing and assessments. We have become the trusted cyber security advisor to leading global organizations.

HolistiCyber does not stop with cyber security-We deliver nation-state level cyber defense to the private market.