Holistic Risk Assessment

Improve business productivity. Protect your company assets.

What is the Holistic Risk Assessment service?

Our holistic risk assessment service is a unique program designed to assess and control cybersecurity risks so that regardless of the evolving cyber threat landscape, the organization's productivity increases and its assets remain secured. The program proactively evaluates systems, applications and processes; and provides clarity on vulnerabilities as well as an effective risk mitigation plan, thus reducing chances for data breaches and business downtimes. **The goal is to mature the organization's security program and elevate its overall security posture.**

What does my assessment include?

1. Mapping organizational roles and responsibilities.
2. Reviewing key security documentation and policies in the context of protecting against cyber threats.
3. Reviewing organizational procedures in the event of a cyber-attack.
4. Mapping information security processes in general.
5. Analyzing relevant constraints such as regulations, structural and operational processes, costs and efficiencies for the enterprise.
6. Testing the integrity of the organization's crucial applications and their effectiveness at preventing cyber-attacks.
7. Assessing the effectiveness of the organization's physical security in relation to sensitive IT systems and potential cybersecurity risks.
8. Includes full network security, mobile security and cloud security assessments.
9. Performing White, Gray and Black box pentesting, vulnerability, and wireless assessments.

WHAT SHOULD YOU EXPECT?

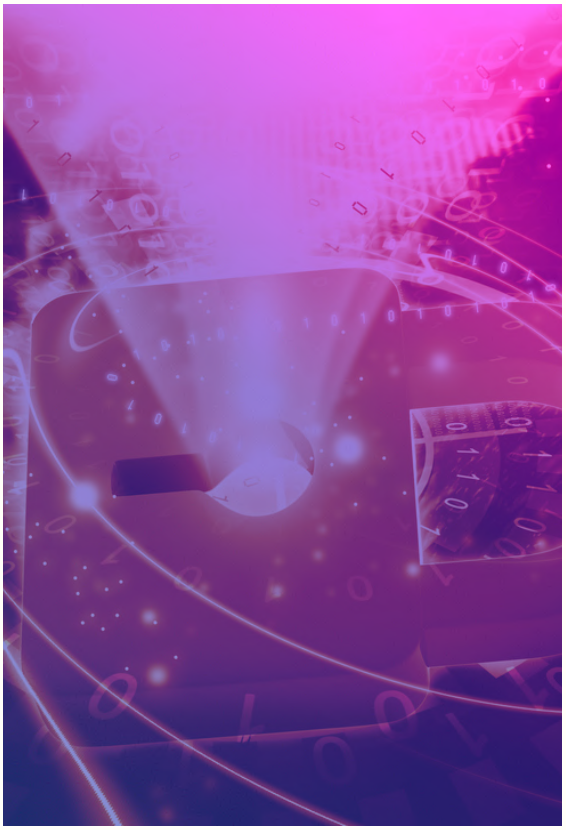
- **Tailored and scalable risk assessment program.**
- **Zero overhead for clients, fully managed service.**
- **Policy outline adapted to unique company business needs, priorities and risk appetite.**
- **Maturing organizational cybersecurity program in consideration of business requirements, workflows and priorities.**
- **Assessing key vulnerabilities and strengths - identifying threats and vulnerabilities that are relevant to your specific assets and their potential impact and damage as well as the strong areas.**
- **Implementing effective risk controls.**
- **Clear prioritization of security threats that need to be handled immediately vs. items that do not pose an immediate risk.**
- **Streight-forward remediation and mitigation tactics and workflows.**

How does this service work for me?

Here is what we typically recommend:

1. Creating strategy for **closing security gaps** along with a **clear priority list**.
2. Establishing **comprehensive security policies** and procedures for the company in consideration of business priorities and cyber-risk appetite.
3. **Managing integrations** needed for the organization to be ready to implement the new policies.
4. **Continuous monitoring** throughout the business relationship to check for cybersecurity gaps.
5. **Scalable and continuous** reporting on changing risk levels, fine-tuning and scaling the strategy as needed.

How can enterprises keep up with today's cybersecurity risks? By getting ahead of them.



In recent years, there has been a quantum leap in the development of tactics, techniques, and procedures of powerful cyber-attack weapons and purchasing such instruments on the darknet has become very easy and fast. In the past, only nation states had access to such weapons, but today various cyber criminal groups have access to these nation-state grade cyber-attack tools and they are using them thousands of times, every day, for financial gain, which has created a new level of risk for the enterprise.

The cooperation between these groups has increased, and so knowledge and tool sharing make it more likely that many more companies will experience a nation-state grade attack.

To address these risks, HolistiCyber provides a tailored and fully managed service that covers all aspects of the cyber kill chain, but in a method that is specific to each company's risk tolerance, business needs, workflows, threat-landscape, and in consideration of attackers' motivations.

For many companies, cyber risk assessments (proactive audits) have become a compliance requirement, a tick-box exercise demanded by regulators and customers, rather than what they should be - **a crucial tool to assure business productivity and bolster an organization's cybersecurity state.**

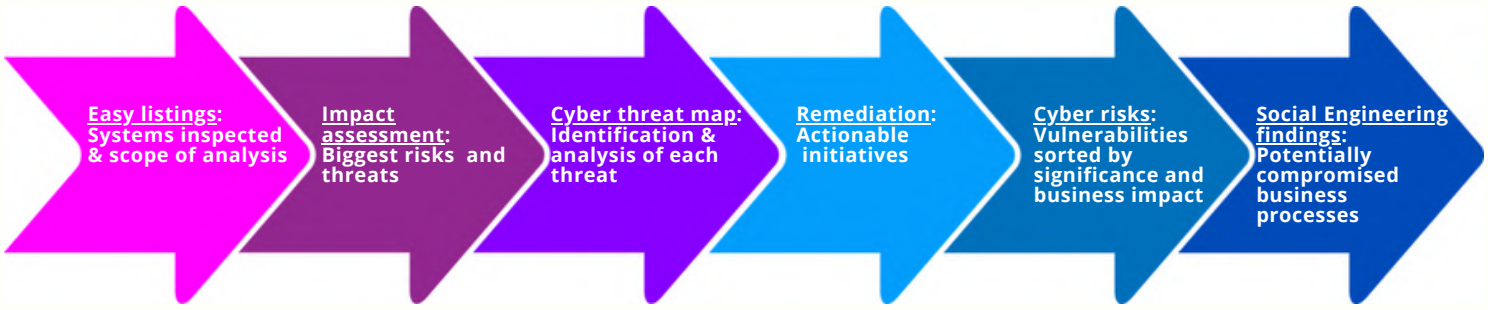


Figure 1: Holistic Risk Assessment Deliverables

Why HolistiCyber?

1. **Nation-state grade expertise** - our staff of white-hat security experts are former military and government offensive practitioners who can examine the attack surface from the **vantage point of the attacker** and not only from the vantage point of the company. This includes a solid grasp of the **sophisticated tooling** available to today's attackers along with access to those attack tools.
2. **Holistic approach** - remediation and mitigation solutions are tied to each company's unique business objectives and workflows. Security should compliment productivity and growth and avoid hindering it.

"HolistiCyber's comprehensive risk assessments and remediation gave us a chance to strengthen our security measures and increase business efficiencies in our security processes. We are continuing to build a robust security program that suits our business needs."

CISO, large manufacturing enterprise, USA