HACKER COMBAT
COMMUNITY

# Cyber Security Risk Assessment: Step-by-Step Guide

# Getting Started on a Risk Management Framework

Cybercriminals design sophisticated attacks on the cloud infrastructure daily. Risk profiles must be created when organizations are adopting containers.

The risk profile should contain the types of threats and vulnerabilities that are expected when it happens. This analysis is very important with containers.

While the level of security visibility over the hosts, containers, and the infrastructure control plane decrease, the attack surface significantly grows.

But the attacks can be avoided when you aim to follow the five steps to create a cybersecurity risk assessment.

You can predict which area of your endpoint system may be vulnerable and develop the security strength of your system's security just before a cybercriminal gets the chance to attack your endpoint system.

# Establish a Baseline of Your "Normal" Operating State

This may be a tricky task if you are only starting or not an IT expert. You may have to ask for an assistance from your trusty IT company staff.

You and the IT team can collaborate to assess the systems, applications, and services as well as scripts that may run in your environment.

Get some help to understand what are the technicalities of your environment.

You should also know how and where the data is flowing.

# Know the Existing Threat Landscape in Your Organization

It is crucial to keep track of the probable threats that are commonly included in risk assessment.

These are insider threats such as malicious or intentional, data leaks with unintentional exposure of information, or data loss.

It depends on your systems, stakeholders, and environments, you will probably discover additional threats. You should take that in mind and include that in your assessment.

Penetration testing with zero knowledge can help your team understand your system's vulnerabilities from an outsider's perspective.

# Define the Ingrained Business Risk and Impact

Have you previously experienced a cyber threat in your system? You have to rate how much impact it cost your landscape without acknowledging the control environment you have.

The assessment can be approached this way to avoid factoring in controls that could moderate the risk. This provides a clear understanding of the full potential of threat events.

*How do you rate the impacts of the threat events? Here are the steps used by SANS that you can incorporate to your risk assessment*

**Minor Severity (Rating 1):** Vulnerability requires few resources to exploit, with little potential for loss. Exposure is relatively insignificant. The effects of the vulnerability are tightly contained, and it does not increase the probability of additional vulnerabilities being exploited.

**Moderate Severity (Rating 2):** Vulnerability needs vital resources to exploit, with significant potential for loss. Or, it requires few resources to exploit, with moderate potential for loss. Exposure is moderate, meaning that one or more system components may be affected. Exploitation may lead to further vulnerabilities.

**High Severity (Rating 3):** Vulnerability requires fewer resources to exploit, with significant potential for loss. Exposure is high, with the vulnerability affecting the majority of system components. There's a significant probability of further vulnerabilities.

# Keep Your Control Environment in Mind

In order to adequately assess your control environment, you need to examine several categories of information.

Most importantly, identify threat prevention, mitigation, detection, or compensating controls and their connection to identified threats.

A few cases of this involve organizational risk management controls, user provisioning controls, and administrative controls.

# Can You Estimate How Prepared You to Compare Businesses?

Lastly, you have to consider the industry sectors in which you and your customers operate and the types of data that you store.

The size of your store, infrastructure, and assets are also very important.

Those components grant you the ability to compare yourself to similar businesses and prepare for threats they have encountered in the past.

HACKER COMBAT COMMUNITY

Regardless of their **risk profiles** or size, all companies should build a foundation of cybersecurity risk management based on good business principles and best practices.

**Follow us**

**Visit**
Hackercombat.com

# Take Charge of Your Security Risk Assessment Now

Another set of security infrastructure is produced with the quick rise of containers and orchestration tools. A good understanding of your organization's specific risks will help you determine where your system needs the improvement.