# Ransomware Gap Assessment (RGA)

## RGA leverages NISTIR 8374 assessment guidelines for identifying ransomware risk.

## Overview

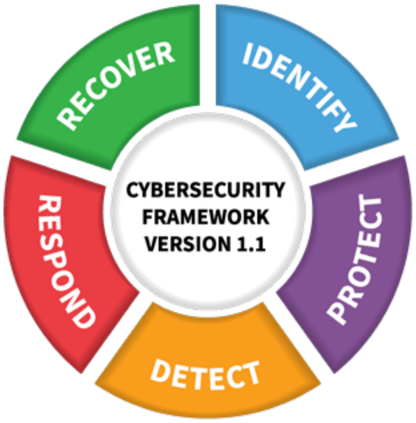
The Ransomware Gap Assessment (RGA) identifies security objectives from the NIST Cybersecurity Framework (NISTIR 8374) that support preventing, responding to, and recovering from ransomware events. The RGA will provide recommendations to reduce the risk of ransomware events. This includes helping to gauge an organization's level of readiness to mitigate ransomware threats and to react to the potential impact of events.

TorchLight consultants will review security posture information, security documentation, and provide the organization with a detailed questionnaire to analyze how existing technologies and business processes address ransomware threats.  The consultants will also conduct interviews with internal stakeholders to ensure that guidance and recommended remediation tasks are aligned with business objectives.

The deliverable of this engagement is a report that details the organization's security posture relative to ransomware threats, as well as move-the-needle recommendations designed to provide the greatest possible threat reduction with the most efficient use of resources.

### Outcomes for the client utilizing NIST guided Ransomware Gap Assessment include:

- The Ransomware Profile aligning ransomware prevention and mitigation with elements of the Cybersecurity Framework.
- Identifying and prioritzing opportunities for improving ransomware resistance.
- Delivering timely, accurate, and economical information so you can proactively get in front of problems.



# Based on NIST Guidelines

Ransomware is a type of malicious attack where bad actors encrypt an organization's data and demand payment to restore access. In some instances, attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. This Ransomware Profile identifies the Cybersecurity Framework Version 1.1 security objectives that support preventing, responding to, and recovering from ransomware events. The profile can be used as a guide to managing the risk of ransomware events. That includes helping to gauge an organization's level of readiness to counter ransomware threats and to deal with the potential consequences of events.

Used in cyberattacks that can paralyze organizations, ransomware is malicious software that encrypts a computer system's data and demands payment to restore access. To help organizations protect against ransomware attacks and recover from them if they happen, the National Institute of Standards and Technology (NIST) offers simple tips and tactics.

NIST's advice includes: Use antivirus software at all times — and make sure it's set up to automatically scan your emails and removable media (e.g., flash drives) for ransomware and other malware. Keep all computers fully patched with security updates. Use security products or services that block access to known ransomware sites on the internet. Configure operating systems or use third-party software to allow only authorized applications to run on computers, thus preventing ransomware from working. Restrict or prohibit use of personally owned devices on your organization's networks and for telework or remote access unless you're taking extra steps to assure security.

NIST has also published more detailed fact sheets on how to stay prepared against ransomware attacks. You can find this material and more on ransomware at the NIST and CISA websites.

## Ransomware Boom!

- In May 2021, Colonial Pipeline, the largest pipeline system in the United States, was ransomware attacked resulting in them paying **$4.4 million**
- The average ransomware payment rose **33%** in 2020 over 2019, to **$111,605**.
- In 2020, ransomware attacks on average caused **18 days** of downtime for the affected companies while the average ransom amount increased by twofold and amounted to **$170,000**.
- Ransomware attacks grew **150% (Varonis)**