CYBER EXTORTION STOPS HERE.

Assess, Recover, and Protect with Anti-Ransomware Services by Edgeworx Solutions Inc.®

Today's ransomware is morphing at a rapid pace—targeting victims without discrimination or notice. Typically distributed through social engineering schemes, the many variations of malware act to infect end-user desktops, servers, and mobile devices to encrypt critical files and systems until the ransom is paid. Without any guarantee of restoring all or even part of the data, the impact cripples businesses for days, months, or even closes the doors permanently.

DON'T LET RANSOMWARE DECIDE YOUR FATE

Under attack or seeking to improve security with proactive defense measures? Edgeworx Anti-Ransomware Services implement business-driven security practices to protect your company's reputation, finances and business operations.

Using industry frameworks, Edgeworx delivers a quantitative report on potential susceptibility to ransomware attacks, including pinpointing areas of weakness that could be exploited. Our customized service assesses your organization's ability to withstand an attack and preparedness to recover by analyzing:

- Administrative Permissions
- Information Security Policies
- Patch Status
- Backup and Restore Plans
- Network and Database Configurations
- System Dependencies
- IT Infrastructure Security Software

During an attack, Edgeworx works expeditiously to handle the entire incident lifecycle. Using sandboxing and other advanced detection techniques, we identify and quarantine even the most evasive infections—preventing ripple effects through the network and endpoints. We aim to get you back to business quickly by:

- Using up-to-the-second intelligence
- Completing a deep-scan on all IT connected devices for malware
- Enacting decryption keys
  Restoring from backups

Post-incident, criminals will be left empty-handed while you receive a report detailing all technical aspects of the attack, including the root cause for future mitigation and protection planning.

Prevention with off-the shelf cybersecurity products is not enough. It requires implementing an ongoing multi-layered defense strategy to achieve effective security. Our custom engagements include:

- Advisement on specific information security policies and configurations of associated technologies that protect investments from increasingly complex threats
- User security awareness training
- Ongoing security assessments (i.e. phishing campaigns, 24/7 security scans, threat monitoring, and next-gen firewalls)

$1,077 USD
Average Ransom Demand in 2018

$75+ BN
Annual Cost of Ransomware

40 SECONDS
Frequency of Ransomware Attacks

67%
Ransomware Victims Permanently Lost Part or All of Their Corporate Data

WAR CHEST SHOULDN'T BE A COST OF BUSINESS

Ransomware perpetrators target victims using two methods:

1. Casting wide nets
2. Targeting small- to medium-sized businesses with IT security loopholes, valuable data, and budgets to pay the ransom

Too many businesses rely on war chests to bail them out of security nightmares. When data is the lifeblood of your operations—and it always is—paying the ransom seems like the best option. Without a guarantee of returning to business as usual, tapping into a war chest only feeds profit-hungry criminals and motivates the next attack.

Edgeworx helps businesses recover quickly and easily without paying by:

- **Assessing** the ransom note to determine a known variant
- **Containing** the threat by deploying system-specific mitigations to protect any further spreading
- **Remediating** with data backups and (where applicable) decryption keys
- **Strengthening** your IT security posture to protect from future attacks

DATA BACKUPS AND FIREWALLS AREN'T ENOUGH

Data backup and recovery, along with detailed security policies, are best practices to ensure your network is protected from the onslaught of cyber security attacks. But what happens when firewalls are breached and backups are encrypted? Together, we help you close any IT security loopholes without productivity repercussions that are commonly associated with multi-layered defense. Our team of experts will consult with you on:

- Information Security Policies
- Penetration Testing
- Phishing Simulations & Training
- Compliance Metrics
- Security Insurance
- State-of-the-Art Defense Technologies
- 3-Stage Backup Methodologies

WHEN THE WORST HAPPENS — COUNT ON EDGEWORX.

Hit by a ransomware attack? Edgeworx will deploy a team of experts to investigate, remediate, and get you back to business—fast.

First, take these steps:

1. Do **NOT** pay the ransom
2. Unplug computers from the network
3. Call **+1.647.793.4731** to speak with one of our team members

edgeworx
Delivers IT visibility

To learn more about Edgeworx, please visit us at edge-worx.com, and follow @Edge_worx on Twitter.

Contact us: 500 Cochrane Drive, Suite 5, Markham, ON L3R 8E2 | +1 (647)-793-4731