SERVICE OVERVIEW

RANSOMWARE READINESS ASSESSMENT

Ransomware attacks are on the rise. Unprepared victim organizations often have to choose between the high cost of recovering crippled IT environments or paying ransom at the expense of reputation. A better option is to get prepared now.

online business systems

Are you prepared for a Ransomware attack?

Do you have a well-defined Ransomware Recovery Plan?

A Ransomware Readiness Assessment helps organizations strengthen their processes and technology to mitigate the threat of Ransomware. Online's team will evaluate the effectiveness of your technical security controls and operational capabilities in responding to and recovering from a ransomware incident.

Our Ransomware Readiness Assessment is a quick way to:

- Gain visibility to the weaknesses in your environment - technology and processes.
- Understand your current response capabilities.
- Identify areas for improvement in recovery.

What We Examine

During our Ransomware Readiness Assessment, we review how you handle:

> M365 Configuration

> Backup and Recovery

> Critical Assets/Data/Segmentation

> Logging and Monitoring

We will also complete:

> IR Tabletop Exercise

> Phishing Exercises

> External and Internal Penetration Testing

Benefits of Conducting Ransomware Readiness Assessments

- Understand your organizational contextual readiness to ransomware attacks.
- Determine if your existing investments and your current processes and procedures enable recovery.
- Identify improvements in your technology, policies and processes.
- Know if your ransomware readiness aligns with your organization's threats, threat actors and risk mitigation strategy.
- Receive specific recommendations on technical aspects, policy and processes to boost detection and response capabilities.

Our Approach

We take a three-phase approach to all of our Ransomware Readiness Assessments. These phases allow us to assess your environment through discovery and then dive deeper into relevant areas as needed.

PHASE 1

Discovery

KEY ACTIVITIES

- M365 Assessment
- Review Backup Plan & Recovery Strategy
- Review critical assets/data segmentation

PHASE 2

Defense Assessment

KEY ACTIVITIES

- Segmentation recommendations, patching, privileged user accts, A/V technology and MS License scheme
- IR Plan/Recovery Review
- Logging/Monitoring/MSSP - Review Custom Use Cases

PHASE 3

Simulations

KEY ACTIVITIES

- IR Table Top Exercises
- Phishing Campaigns
- Penetration Testing

Contact:
Online Business Systems
1.800.668.7722
rsp@obsglobal.com

About Online Business Systems

Online is a leading Digital Transformation and Cybersecurity consultancy. Businesses today are under pressure to transform to remain relevant – at the same time, there is unprecedented opportunity to innovate and achieve incredible things never seen before – securely. We combine the best technology, business, and security practices, and lead Clients through the transformation process.