

► Ransomware Preparedness Services



Reduce the risk of criminals succeeding with ransomware attacks. Now is the time to prepare your company before the attack hits.

In this day and age of ransomware attacks, a commitment to cyber hygiene and best practices is critical to protecting your networks. A complete Ransomware Maturity Assessment will help you systematically understand your organization's current security state and provide a roadmap for strengthening your processes and technology to mitigate the threat of ransomware.



► Ransomware Maturity Assessment

AccessIT Group's Ransomware Maturity Assessment focuses on three key areas, –Prevention, Segmentation and Limiting the Spread of Ransomware, and Incident Response– which are designed to help your security team identify deficiencies and minimize your organization's overall attack surface.

- **Prevention**–Determine your organization's ability to minimize its attack surface or stop ransomware from occurring
- **Segmentation and Limiting the Spread of Ransomware**–Determine your team's ability to detect, contain or limit the impact of an attack
- **Incident Response (IR)**–Identify any deficiencies during the incident and recovery period

Our security consultants will help your team prepare and respond quickly to a ransomware attack so that your organization is in the best possible position to protect its network, operations and data.

► IR Plans and Ransomware Playbooks

Does your incident response plan include what to do during a ransomware event? The faster your organization can recover from a ransomware attack, the better. A proactive Incident Response approach will help your team make speedier decisions in the event of such an attack and help you get back up running quickly following the event.

As part of this exercise, AccessIT Group's security risk advisors will interview your organization's stakeholders to collect information on your people, processes, and technologies to garner a full picture and provide you with a customized Incident Response Plan and Ransomware Playbooks.

Our methodology in helping clients develop or validate an IR plan incorporates both our experience in responding to persistent and emerging threats and guidance from leading security standards, such as the NIST Cybersecurity Framework and CIS Controls™.



► Ransomware Preparedness Services



► Ransomware Tabletop Exercises

When it comes to playing chess, you might think you have a solid strategy but without practice it is likely that you won't win a lot of games. Why should ransomware recovery be any different?

A ransomware tabletop exercise is an excellent way to prepare your team for the real-time aspects of a cybersecurity attack and ensure they have the right skills to handle an attack.

Our security consultants will facilitate simulations and discussions to determine the team's readiness and identify potential gaps. Following the exercise, they will provide guidance and recommendations on the response process:

- Preparation
- Detection and Reporting
- Triage and Analysis
- Containment and Neutralization
- Post-Incident Activity

► Access Control Assessment

Taking steps to reduce the damage that a hacker can do if they breach your defenses is essential. Preventing lateral movement from within your network is one important way to minimize damage.

AccessIT Group's security professionals will examine your network and recommend and implement technologies that provide deep visibility into your attack surface and evaluate deficiencies, as well as provide remediation recommendations to:

- Mitigate existing threats
- Maintain hardened security
- Detect actual attacks in progress
- Investigate incidents and hunt for threats



Leverage our experienced team to identify and eliminate weak points within your infrastructure to improve your overall security posture.



www.accessitgroup.com
866-748-AITG (2484)