

THE NEED FOR RANSOMWARE READINESS

One in five businesses that pay ransom will never recover their data.

The increasing severity and frequency of ransomware attacks drives a critical need for businesses to develop reliable prevention and mitigation plans.

The Chertoff Group's Ransomware Readiness Assessment (RRA) is a one-week program that assesses an organization's current anti-ransomware measures, identifies gaps and vulnerabilities in prevention strategies and proposes immediate, actionable steps for rapidly reducing risk and designing for resiliency in the event of an attack.

The RRA Process Includes:

- Up to three days of on-site assessment of current ransomware protection, management and response capabilities designed to identify and address system gaps and vulnerabilities.
- Collaboration with the organization's primary contacts in IT operations and security, senior technology and security leadership (i.e., CIOs, CTOs, CSOs and CISOs) and other individuals involved in network management and incident response.



OUR DIFFERENTIATOR

**OUR SECURITY EXPERTS
WORK **ONSITE** WITH
YOUR IT AND SECURITY
TEAM TO PREVENT
RANSOMWARE**

RRA Results and Deliverables:

- A focused, actionable assessment of the organization's cybersecurity capabilities and the most effective means of ransomware protection, response and recovery.
- Practical recommendations for the security team delivered in real time and customized to each client's preferred risk management standard.
- A report of findings and recommendations presented to IT operations and security teams.
- No mandatory follow-up. However, The Chertoff Group will extend a standing offer for continued assistance and engagement.

Who Can Benefit From an RRA?

Our RRA is most popular with small to mid-sized businesses, but is easily scalable; organizations of all types and sizes can benefit. The RRA is especially applicable to businesses that:

- Have smaller IT operations and security staff.
- Are consumed with day-to-day management and view security as a secondary priority.
- Do not feel fully prepared to prevent and respond to a ransomware attack.