TheChertoffGroup
Enabling A More Secure World

RANSOMWARE READINESS ASSESSMENT FAQ

The following FAQ provides a high-level overview of The Chertoff Group's Ransomware Readiness Assessment (TCG RRA).

WHAT IS RANSOMWARE?

Ransomware is technically defined by US-CERT as "a type of malicious software (malware) that infects a computer and restricts access to it until a ransom is paid to unlock it."

HOW PREVALENT ARE RANSOMWARE ATTACKS?

- Ransomware attacks have increased dramatically in recent years, crippling business operations unless and until payment is made to the attacker.
- Attackers can have different objectives. Some aim only to disrupt, while others seek a payoff. A number of major global companies were impacted by notPetya, a ransomware campaign originating in Ukraine in June 2017, with impacts at one company running over $750 million.

WHAT IS THE CHERTOFF GROUP'S (TCG) RANSOMWARE READINESS ASSESSMENT (RRA)?

TCG RRA provides a rapid evaluation of an organization's cybersecurity capabilities, with a particular focus on ransomware's impact on the integrity and availability of critical systems and data. TCG RRA:

1. Validates the extent to which key risk-reducing controls are established and/or supplemented by operational security measures.
2. Offers advice on immediate risk-reducing steps for identified gaps.
3. Provides sample metrics for ongoing performance monitoring.

WHAT IS ITS PURPOSE?

TCG RRA gives organizations an immediate snapshot of their ransomware susceptibility and provides practical steps to risk reduction.

HOW LONG DOES TCG RRA TAKE?

The assessment is expected to last one week or less, depending on security team availability, with two to three days of on-site work, follow-up, virtual discussion and final wrap-up.

WHERE DOES TCG RRA TAKE PLACE?

The review is expected to occur two to three days at the facility housing the customer's primary security functions, with the remainder conducted remotely as required.

WHAT IS THE SCOPE OF TCG RRA?

The team uses a ransomware "Threat Pathways" analysis (e.g., "Package & Delivery, Load & Run, Encryption & Replication, Ransom & Extortion") to evaluate a client's defenses against ransomware incidents. We call it the ***Ransomware Threat Pathways Analysis.*** Key components include:

- *Defenses to limit initial infection*
  - Asset management (risk-based)
  - Configuration management (risk-based)
  - Vulnerability management (risk-based)
  - Email management
  - Web browsing management
  - Web application management
  - Anti-malware tool management
- *Defenses to limit internal spread*
  - Segmentation
  - Configuration management – internal resources
  - Vulnerability management – internal resources
- *Defenses to detect and respond to ransomware incidents*
  - Detection & response
  - Third party resources
  - Crisis management considerations
- *Defenses to enable rapid recovery*
  - Business impact assessment
  - Process for backups
  - Disaster recovery planning & testing

WHAT DOES THE ON-SITE VISIT INCLUDE?

- A possible on-site schedule might cover the following areas (as applicable):

  Day 1: Review email systems, web browser, web server configurations, web application security, anti-malware capabilities, approach to vulnerability management (including external/internal scanning and patch management), DNS filtering and user awareness/phishing, whitelisting and segmentation.

  Day 2: Review detection and response capabilities, third-party resources, crisis management considerations, business impact assessments and data backup/recovery.
- The Chertoff team both reviews the capabilities in place and works with the security team to help them better understand and address identified gaps and issues.

WHOM WOULD TCG MEET DURING THE ASSESSMENT?

- TCG would expect to meet, at the least, primary points of contact (POCs) in IT operations and security, senior leadership in the technology and security chains of command (e.g., CIO, CTO, CSO, CISO, etc.), and individuals with specified roles in incident response.
- TCG may need to meet significant security vendor POCs, like MSSP representatives and others, with the initial meeting happening on-site (if at all possible) and subsequent visits held virtually.

WHAT DO I RECEIVE AT CONCLUSION OF THE REVIEW?

- TCG RRA provides the customer organization a "hands-on" review and relays recommendations in real time to the security team.
- This occurs both while the Chertoff team is onsite, working directly with the company's IT and security professionals, but also during follow-up sessions as needed.
- A final report summarizes what was discussed and relayed to IT operations/security team during the engagement in PowerPoint presentation structured around a risk management framework and Ransomware Threat Pathways approach.
- Typically, the team would hold a final, virtual outbrief with identified POCs to review the conclusion of the engagement and the report and answer any remaining questions.

HOW MUCH DOES IT COST?

- **The Chertoff Group Ransomware Readiness Assessment price will be contingent on the size and complexity of the client environment.**
- The offering encompasses an onsite assessment, coordination with/instruction for the security team and tool tuning recommendations.
- A summary report of findings and recommendations will also be provided soon after completion of the engagement.
- For a to-be-determined additional fee, organizations can request a more comprehensive report containing greater detail on findings and more in-depth remediation recommendations.

WHY SHOULD I WORK WITH TCG?

- The Chertoff Group approach is different because we begin by considering an organization's business objectives and then assess the extent to which the security program is effectively designed and implemented to advance these objectives now and as they evolve.
- Security is about risk management, not risk elimination. The Chertoff Group is an advisory firm comprised of experts with decades of accumulated experience helping clients understand and manage security risk across physical and cyber domains, and build resilient organizations.
- We apply an offense-informed defense analysis to assess technology environments from the mindset of an adversary.
- We are one of the only consulting firms in the world with Department of Homeland Security SAFETY Act designation, establishing our Security Risk Management Methodology as effective in reducing security risk.
- We work to reflect the changing nature of inherent risk in program design, and our methodology also accounts for implementation risks so organizations avoid trip-ups as they build their programs.
- Our approach works to prioritize preventive measures based on risk. We also assume that an incident will happen, and we work with clients to design for resiliency.
- We stress the importance of testing and continuous monitoring of mitigation measures to demonstrate effective security performance.

Contact **info@chertoffgroup.com** to schedule an assessment.

TheChertoffGroup
Enabling A More Secure World

WWW.CHERTOFFGROUP.COM
1399 NEW YORK AVENUE, NW, SUITE 1100 | WASHINGTON, DC 20005
T. 202.552.5280 | F. 202.330.5505 | WWW.CHERTOFFGROUP.COM