# SERVICE BRIEF FOR
# RANSOMWARE READINESS ASSESSMENT

Lodestone's Ransomware Readiness Assessment prepares your company to face off against the increasing prevalence of ransomware threats by identifying where your defenses are strong and where vulnerabilities exist. Ransomware is a type of malware used to encrypt files from a victim's environment, effectively locking them out of their own data. This is often preceded by data theft and followed by ransoms from the threat actor, where payment is demanded in exchange for decrypting the files or preventing the public release of stolen data.

In both the media and practice, ransomware has become a growing threat faced by businesses in every industry. Our engineers go beyond phishing, vulnerable access protocols and services, and remote management and monitoring to assess your organization's tools, procedures, and overall ability to respond to and mitigate this specific type of incident.

## BENEFITS

- The peace of mind that comes with preparation and a strong security posture that we will help you achieve through assessing your current defenses and creating a game plan to close any gaps and address vulnerabilities.
- Empowering your personnel as the first line of defense against common threat actor tactics, including those for ransomware, such as social engineering and phishing.
- Demonstration of your organization's commitment to protecting your customer's data and your reputation and the ability to stand against a type of incident that costs businesses hundreds of thousands of dollars each year.

## OVERVIEW

Lodestone's Ransomware Readiness Assessment evaluates your organization's readiness to combat a ransomware attack. We will assess the processes and technologies currently in place to mitigate the threat and suggest applicable improvements. This will include the following areas:

- External Testing – Identifying any externally-facing assets or vulnerabilities that could be leveraged during a ransomware attack.
- Human Aspect – Evaluating the susceptibility of your organization's users to phishing attacks, a popular ransomware attack vector.
- Assumed Breach Testing (Internal) – Determining if controls currently present (e.g., SIEM, DLP) in your internal network can respond optimally and appropriately should a threat actor infiltrate your environment. This includes assessing the internal network for existing vulnerabilities.
- Encryption – Identifying weaknesses in detection and the protection of endpoints by simulating a ransomware infection.

## WHY LODESTONE

Lodestone is a global cybersecurity firm committed to helping clients prevent, investigate, and prepare for security incidents. It was built from the ground up to offer an innovative, behavior-based approach to proactive cybersecurity and digital forensics and incident response (DFIR). We are comprised of top investigative talent and offensive security experts from several of the world's largest cybersecurity firms, as well as military veterans and former members of national security organizations, including the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA). We combine this expertise with our unique understanding of legal requirements through our relationship with our parent company, Beazley, which has been at the forefront of cyber insurance for over a decade. Through this relationship, Lodestone has developed a unique understanding of the intersection between insurance and cybersecurity while preventing, preparing for, and responding to some of the toughest security challenges that industries face today.

### Compliance

Since its founding as a subsidiary of Beazley in 2017, Lodestone has offered its customers insight into both cybersecurity and the cyber insurance industry. We help companies align and stay compliant with cyber insurance coverage requirements. In addition, we offer discounts to channel partners to form long-term relationships.

### Security Focus

Lodestone's experts live and breathe cybersecurity and are committed to helping customers face some of the biggest challenges of their careers. We do not sell vendor security products – our offerings are purely service-focused, and any third-party tools we recommend are the product of genuine, vendor-agnostic, and tested endorsement, not business deals.

### Expertise

Lodestone's approach to Incident Response is to have the top cybersecurity experts in the world, as the lead, and as the touchpoint, when responding to cybersecurity incidents. This is done with the backing of comprehensive, real-time threat intelligence to provide clients with protection across the life cycle of a potential security event or incident.

### Tailored Approach

We understand the individual challenges of every situation and consider the human side of the equation, never taking a "one size fits all" approach. We blend design, threat intelligence, and technology with human insights to provide clients with the greatest cybersecurity advantage.

### Threat Intelligence

Our deep understanding of threat actor tactics, techniques, and procedures (TTPs) is based on decades of experience in DFIR and the diligent gathering of threat intelligence from all possible sources.

### Agility

Time is of the essence before, during, and after an intrusion. We stand ready to move in quickly and effectively at the first sign of an intrusion.

### Team Experience

**1000+**
**ENGAGEMENTS**

**200+** YEARS
**COMBINED EXPERIENCE**

**50+**
**CERTIFICATIONS**

### Experts Unlike Anyone Else

**EX-**

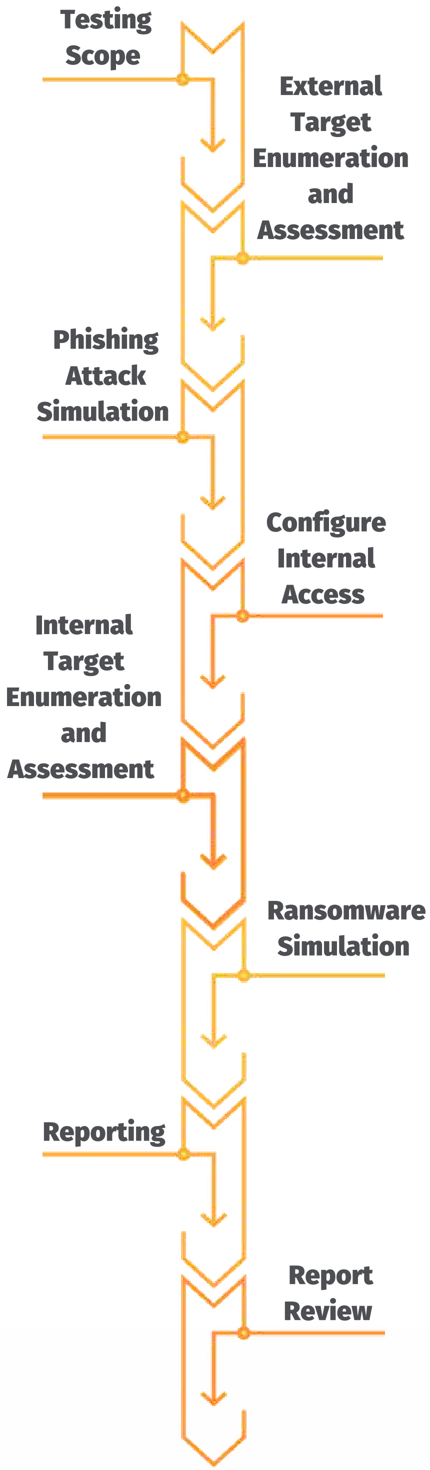
MILITARY
LAW ENFORCEMENT
INTELLIGENCE
TOP CYBER TECH
TOP CONSULTING
FORTUNE 100 ENTERPRISE

### Global Presence - NA/Europe

## METHODOLOGY

Lodestone’s Ransomware Readiness Assessment aims to simulate an increasingly common real-world attack scenario to provide visibility into your organization’s readiness for ransomware attacks. The goal of the assessment is to understand whether implemented tools, technologies, and procedures can identify activities related to ransomware activities and what action they take upon identifying it.

The phases of this assessment are as follows:


Testing Scope
External Target Enumeration and Assessment
Phishing Attack Simulation
Configure Internal Access
Internal Target Enumeration and Assessment
Ransomware Simulation
Reporting
Report Review

- Testing Scope – Lodestone will work with you to understand your environment and determine the best course of action for assessing your internal and external infrastructure, including areas to be excluded from testing.
- External Target Enumeration and Assessment – Our engineers will gather information of all types on your organization to develop a footprint similar to a threat actor preparing to launch an attack. This footprint will be used to identify misconfigurations and vulnerabilities in the external infrastructure.
- Phishing Attack Simulation – We will craft a custom phishing attack that tests the susceptibility of your organization's users to a popular ransomware attack vector without any risk to your business.
- Configure Internal Access – Lodestone will use an assumed breach paradigm to assess the internal client environment's susceptibility to a threat actor that was able to enter the environment. Access may be provided either via a payload used in the previous phishing attack simulation step, a dedicated instance of client-owned hardware, or by simply giving access to client hardware to test from.
- Internal Target Enumeration and Assessment – Our engineers will enumerate assets within your internal environment. This includes looking at file sharing and other services present within the environment that could support the spread of ransomware. Should the internal network be compromised, do the controls present (e.g., SIEM, DLP) in the internal network contain the breach and alert the appropriate personnel?
- Ransomware Simulation – We will simulate a ransomware infection within your environment to provide the most realistic insight into how your company responds to these attacks without the danger of an actual incident.
- Reporting – All findings will be compiled into a cornerstone deliverable that provides meaningful insights into your organization's security posture, especially the human element. Our experts share assessment results that can be used to develop improvements in your technology, policies, and processes.
- Report Review – We provide our clients at least two weeks to review the reports and formulate any questions or requests for clarification. At the end of every engagement, a report review call is scheduled to ensure that all of your concerns are addressed.

## INFORMATION GATHERED

The following artifacts may be obtained from our team as part of the assessment:

- Email list of targeted personnel
- Credentials or other payloads obtained from phishing simulations

## DURATION AND DELIVERABLES

The Ransomware Readiness Assessment varies in duration based on the size of your environment, the number of systems, and findings, but typically takes two to three weeks. It can be delivered on-premises or remotely.

Lodestone will provide the following deliverables to you as part of the engagement:

| | |
|---|---|
| | **Weekly Status Reporting –** Lodestone will provide a weekly or bi-weekly status report to the project sponsor once the kickoff call is complete. Lodestone can accommodate your preferred communications, including via phone call or email. |
| | **Executive Summary Report –** Lodestone will provide a high-level report on the engagement, findings, and any recommendations, if applicable. |
| | **Final Report –** After the engagement completion, Lodestone will provide a final report that details the engagement, findings, and recommendations for mitigating the findings. |

Learn more at www.lodestone.com

Connect with us:

320 East Main Street, Lewisville, TX 75057, USA

Tel: +1-203-307-4984

info@lodestone.com

Lodestone Security is a wholly owned subsidiary of Beazley plc. Lodestone provides computer security and cyber security consulting services. Lodestone does not provide insurance services and client information obtained by Lodestone is not shared with Beazley claims or underwriting. Likewise, client information obtained by Beazley claims or underwriting is not shared with Lodestone.