Lodestone

SERVICE BRIEF FOR

PHYSICAL SECURITY ASSESSMENT

The Lodestone Physical Security Assessment applies an intensive audit structure that addresses your company's physical security. We evaluate existing or planned security measures that protect assets from threats and identify areas for improvement. Physical security protects more than your company's assets, but your company's heart – personnel, hardware, and offices. Ensure that your organization is demonstrating best practices for these crucial defenses.

Our engineers will assess your environment to identify areas where security controls may be weak, missing, or lacking, considering the human, technology, and policy factors. We follow up by walking you through how any gaps may be exploited by a threat actor.

BENEFITS

- Identifying the biggest threats to your people and property paired with expert guidance on spotting and addressing security gaps based on criticality, all without disrupting your daily business operations.
- Support for your IT team and similar groups by prioritizing physical security and providing a clear business case for allocating funding for security improvements.
- Prioritization of physical security upgrades to help your company strengthen its physical security posture with cost-effective strategies that are friendly to budgets.

OVERVIEW

Lodestone's Physical Security Assessment is an intensive audit of your company's current physical controls and the training that your employees have undergone. Our experts use real-world social engineering techniques like tailgating, lockpicking, and RFID duplication to evaluate the overall physical security of your organization.

We examine user interactions, security personnel, and the presence and placement of tools like video cameras, badge readers, and mantraps. After the assessment, we present key wins and areas that need improvement to boost your company's physical security.

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

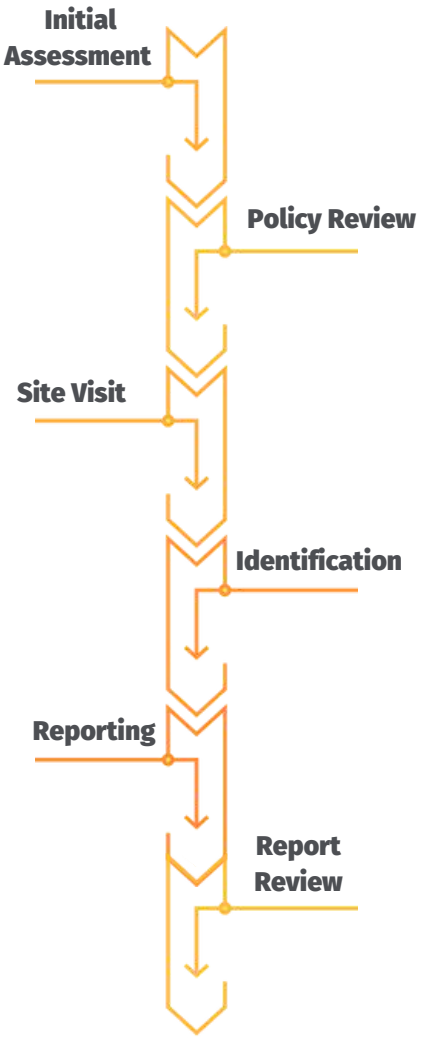
EX-
MILITARY
LAW ENFORCEMENT
INTELLIGENCE
TOP CYBER TECH
TOP CONSULTING
FORTUNE 100 ENTERPRISE

Global Presence - NA/Europe

METHODOLOGY

Lodestone's Physical Security Assessment includes the identification of weaknesses in your environment from a physical perspective. We provide direction on addressing those weaknesses and equip you with a better understanding of assets, vulnerabilities, their severity, and the overall risk.

The phases of the assessment are described in the subsections below.



- Initial Assessment - We work with you to understand your business's unique organization and needs. While any organization is at risk for crime, the likelihood differs, and our engineers stand ready to assist you in deciding whether you should scale your security measures and how.
- Policy Review - Physical security controls are critical, but meaningless if they are not adhered to in daily operations. Our engineers examine your physical site and facilities for implemented physical security controls to identify any insufficiencies or other weaknesses. Lodestone divides into three main categories:
  - Review current site and facility security
  - Review facility operating procedures
  - Review physical security systems
- Site Visit - Our engineers evaluate your company's implemented security controls using real-world techniques while on site at a physical location. This includes attempting to impersonate legitimate employees and using other types of social engineering to gain unauthorized access to various components of your business.
- Identification - Threat actors can easily exploit the vulnerable security controls, including unauthenticated access to the camera systems, unmonitored badging (if applicable), and other systems, especially if they are not up to date. Lodestone experts dive into your environment to catalog your physical security resources and ensure they include the latest patches and updates.
- Reporting - All findings are compiled into a report that describes your organization's physical security posture, especially the human element. Our experts share these assessment results to help you develop or enhance physical security at your company. Lodestone engineers are also available to help you develop your physical security policies, plans, and procedures.
- 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 by our team as part of the assessment:

- List of relevant employees
- Physical control information, including devices in place
- Access to physical devices like CCTV and server rooms, if applicable

DURATION AND DELIVERABLES

The Physical Security 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:

	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

©2022 Lodestone
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.