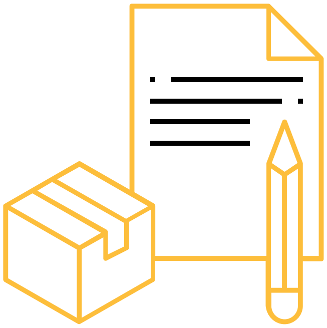
Lodestone

SERVICE BRIEF FOR
INCIDENT RESPONSE PLAN DEVELOPMENT



Lodestones Incident Response Plan Reviews and Development are designed to help organizations create a comprehensive incident response plan that addresses all aspects of incident response, from identification and containment to recovery and post-incident analysis. We work closely with our clients to ensure that their IR plans are easy to understand, easy to implement, and aligned with industry best practices and compliance requirements.

Lodestone leverages direct experience in handling all types of recent cyber-attacks, including ransomware, to ensure that your incident response plan is effective for today's and tomorrow's cyber-attacks.

BENEFITS

- Readiness - you will have a response guide with clear steps to follow in case of a security breach.
- Agility - you will be able to quickly respond to a security incident and significantly reduce damage and downtime.
- Consistency - you will have all your stakeholders on the same page, responding to the breach in a consistent fashion.
- Communication - you will improve communication among stakeholders during a cyber incident.
- Reduced risk - you will identify potential threats and have strategies to mitigate them, therefore improving your organization's security posture and reducing the risk of a cyber attack.
- Compliance - you will be in compliance with many regulations and standards that require organizations to have a cyber incident response plan in place.
- Cost reduction - you will significantly lower the costs associated with a security breach.

METHODOLOGY

Lodestone Incident Response Plan Development service is comprised of these primary phases:

Preparation
Document Review
Policy Development
Delivery and Review
Finalization

- Preparation – We work with you to identify any particular scenarios your organization is concerned about and determine what tabletop exercise or exercises would be performed. In addition, our experts are available to make recommendations based on your industry and other unique factors to determine what scenarios would reflect a security incident your company is most likely to face.
- Document Review – Lodestone experts review your existing documentation, if any, along with any relevant frameworks. We meet with your key personnel to understand how security currently fits into your company’s day-to-day operations, and what level of maturity is needed to suit your needs and meet compliance and regulatory requirements for your business.
- Policy Development – Our seasoned professionals work with any existing documentation and create policies from scratch where necessary to improve your security posture and better adhere to any essential frameworks. These may include the Center for Internet Security 18 (CIS-18), the National Institute of Standards and Technologies (NIST), the Health Information Privacy and Portability Act (HIPPA), and the Payment Card Industry Data Security Standard (PCI-DSS).
- Delivery and Review – The completed policy package is delivered to your key personnel by Lodestone experts and reviewed together to ensure that the documentation meets your needs and suits your organization. This includes a question-and-answer session to provide any necessary clarification.
- Finalization – The policy package is finalized based on feedback and discussions with your organization and the final product delivered.

DURATION AND DELIVERABLES

Incident Response Plan Development varies in duration based on the amount of existing documentation and the complexity of the frameworks and standards that must be met. In general, it typically takes two to three weeks.

As part of the engagement, Lodestone will provide a policy package that contains all policies agreed upon, developed, reviewed, and refined as part of the engagement.