

Incident Response Plan Services

An effective, efficient response to a cybersecurity incident is vital for minimizing organizational risk. Detailed Incident Response Plans (IRPs) are a critical component in managing the response to such incidents.

LevelBlue's methodology and approach

LevelBlue is uniquely positioned to lead the development and enhancement of comprehensive Incident Response Plans as we help clients assess, mitigate, and recover from cybersecurity threats daily.

Aligned with our clients' needs and best practice security standards (e.g., NIST SP 800-61), LevelBlue will review current incident response plans to recommend edits that mature existing processes or collaborate with clients to develop a new incident response plan that drives the incident response program.

LevelBlue understands our clients' time is valuable and, as such, takes a data gathering first approach by requesting and reviewing current documentation, such as policies, standards, and procedures, and conducting information gathering sessions with key stakeholders involved in responding to a cybersecurity incident, such as executive leadership, information security, IT, and legal, within the first week of the project. This approach allows LevelBlue to quickly understand how the organization operates and inform the development of a tailored incident response plan while saving valuable client time.

Over four weeks, LevelBlue will develop a plan that aligns with current stakeholder roles, covers the entire incident response lifecycle, and enhances our clients' readiness to respond to incidents. The plan will include documentation, process templates, and more.

Engagement deliverable options

Incident Response Plan Development:

- Customized

Incident Response Plan Review:

- Recommend IR plan improvement summary report
- Client IR plan inline edits and annotations



