PRIMER

Incident Response Plan

Incident Response Plan Services

An effective and efficient response to a cybersecurity incident is vital for minimizing organizational risk. Incident Response Plans (IRPs) are a critical component in managing the response to such incidents and should include details like roles and responsibilities, escalation procedures, key internal and external contacts, documentation, process templates, and more. Stroz Friedberg is uniquely positioned to lead the development and enhancement of comprehensive Incident Response Plans as we help clients assess, mitigate, transfer, and recover from cybersecurity threats daily.

Stroz Friedberg's Methodology and Approach

Aligned with our clients' needs and best practice security standards (e.g., NIST SP 800-61), Stroz Friedberg 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. Stroz Friedberg 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 Stroz Friedberg 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, Stroz Friedberg 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.

Engagement Deliverable Options

Incident Response Plan Development:
- Customized

Incident Response Plan [DOC] Incident Response Plan Review:
- Recommend IR Plan Improvement Summary Report [PDF]
- Client IR Plan inline edits and Annotations [DOC]

Preparation

Detection and Analysis

Containment, Eradication, and Recovery

Post-Incident Activity

About Stroz Friedberg

Stroz Friedberg, a LevelBlue company, delivers intelligence-driven digital risk management with expert-led services designed for adaptive resilience.

With over 25 years of leading the resolution of the most complex, high-stakes digital risk issues, we manage the entire digital risk lifecycle – from cyber threats and insider risks to IP theft and regulatory compliance. Our approach combines managed security services with expert analysis and strategy, supported by threat intelligence gathered from thousands of engagements across various industries.

We translate complex technical and legal risks into actionable strategies, helping CISOs and legal teams turn digital risks into board-ready insights. Our comprehensive services include managed cyber defense, digital forensics and incident response, trade secret protection, expert witness support, threat intelligence, security strategy and governance, attack path mapping and testing, and resilience engineering.

Operating as one trusted partner, we align technical precision with business priorities to protect critical assets, adapt to evolving threats, and maximize ROI through proven outcomes. Through LevelBlue's portfolio, these specialized services integrate seamlessly with 24/7 managed security operations and AI-driven threat detection for comprehensive digital risk protection.

Cybersecurity. Simplified.

levelblue.com/strozfriedberg