

勒索软件攻击情景方案

面向勒索软件攻击情景的管理层应对与协同支持方案



围绕勒索软件攻击这一关键风险情景，
帮助组织形成更清晰、可执行的管理层应对与恢复思路。

为什么需要这个方案

勒索软件攻击已成为当前组织面临的高影响风险之一。

这类事件往往兼具网络攻击、系统中断、业务停摆、数据风险、舆情压力与外部沟通挑战，对管理层判断、跨部门协同与业务恢复能力提出极高要求。

许多组织虽然已经具备一定的网络安全与连续性管理基础，但在真实勒索软件攻击情景下，仍普遍面临以下问题：

- 攻击事件与业务中断往往同时演化，管理层难以及时形成稳定判断
- 技术处置、业务恢复、对外沟通与管理决策之间缺乏有效衔接
- 现有预案与机制在高压条件下难以真正发挥作用
- 虽有演练，但缺少围绕勒索软件攻击这一关键风险情景的系统化设计与验证

这类风险，不宜仅作为网络安全技术问题看待，而需要围绕具体情景形成更清晰、可执行的应对方案。

适用对象与适用场景

适用对象

- 金融、通信、能源、交通、高科技制造等高连续性要求行业组织
- 高度依赖信息系统、数据与网络支撑的组织
- 董事会、高级管理层、BCM 团队、信息科技与网络安全团队、关键业务与职能部门
- 希望围绕勒索软件攻击建立或强化情景化应对能力的组织

适用场景

- 已将勒索软件攻击识别为关键风险情景之一
- 希望围绕该情景形成更清晰、可执行的管理层应对与恢复思路
- 希望验证管理层、跨部门协同与恢复机制在高压条件下是否真正发挥作用
- 希望将网络安全事件应对与业务连续性和危机管理有效衔接起来

本方案既适用于已有一定网络安全与连续性管理基础、希望进一步深化管理层应对与协同支持的组织，也适用于希望以关键风险情景为牵引推进真实能力与机制建设的组织。

方案目标

本方案通常围绕以下目标开展：

- 识别勒索软件攻击情景下的关键影响路径与主要管理挑战
- 形成管理层视角下整体、可执行的应对与恢复思路
- 提升管理层与关键岗位在高压条件下的判断、授权与协同能力
- 验证现有机制、预案与支撑安排在真实压力条件下的可用性
- 为后续优化组织的连续性能力、治理机制与专项预案提供依据

方案的重点，不只在于“如何处置网络攻击”，
而在于组织如何在高压力条件下保持判断、控制局面并推动恢复。

主要内容

本方案通常包括以下工作内容：

1. 情景界定与重点问题确认

结合行业特点与组织关注重点，明确勒索软件攻击情景的范围、假设与重点挑战。

2. 关键影响与中断路径分析

识别网络攻击事件可能引发的系统中断、业务影响、管理压力与外部影响扩散路径。

3. 应对思路与关键机制设计

围绕决策指挥、事件处置、业务恢复、对外沟通、专业支撑等关键环节，形成整体应对框架。

4. 推演演练与协同验证

通过管理层桌面推演、跨部门联合演练或专项验证，检验关键机制与行动安排的有效性。

5. 评估总结与优化建议

梳理关键发现、能力短板与机制问题，形成后续改进建议。

方案可根据客户需求，侧重于“情景设计”“管理层推演”“跨部门演练”或“能力评估”等不同重点。

交付成果

根据客户需求与实施方式不同，交付成果通常包括：

- 勒索软件攻击情景设计材料
- 关键影响路径与主要管理问题分析结果
- 管理层推演或联合演练方案文件
- 管理层及跨部门应对框架建议
- 演练观察记录、问题清单与评估发现
- 后续改进建议与能力优化方向

可选扩展成果

- 全过程任务框架 / MSEL 设计
- 管理层研判决策支持材料
- 关键岗位职责与协同界面梳理
- 与 BCM、网络安全或危机管理机制的衔接建议

方案特点与价值

本方案的主要特点在于：

- **聚焦关键风险**：围绕勒索软件攻击这一具体关键风险情景展开，针对性强
- **系统完整**：不仅关注技术处置与恢复安排，更重视管理层判断、跨部门协同与整体恢复组织
- **实施方式灵活**：可兼顾情景设计、管理层推演、联合演练、能力验证与机制优化
- **可定制**：可根据行业特点、组织基础与关注重点进行定制化设计
- **灵活可调**：既可单独实施，也可与连续性能力建设、治理机制评估等工作衔接推进

其价值不只在于“做一次演练”，

而在于借助这一高压情景，校准组织在真实中断中的连续性能力与治理表现。

进一步沟通

本方案可根据客户行业特点、组织基础与关注重点进一步细化，并可与以下工作联动推进：

- 管理层桌面推演与情景演练
- 跨部门联合演练与协同验证
- 连续性能力与治理机制评估
- 重大 IT 与数字化中断情景方案
- 关键供应链中断情景方案

欢迎围绕勒索软件攻击情景、管理层应对、跨部门协同与恢复机制建设，进一步沟通交流。

联系方式

网 址： www.xinchangan.cn

电 话： 010 5360 5969 / 130 0109 0810

公众号：bcmplus

