团队工程：业务弹性和网络安全

Linda Laun 2015 年 11 月 18 日

随着科学技术和商业环境日趋复杂，业务弹性面临巨大挑战，这要求组织发展跳出传统业务连续性和风险度量范畴。与此同时，愈发盛行的侵入性安全漏洞和网络犯罪也带来了越来越多的灾备风险。

出现网络漏洞时，企业应制定行动方案，以便业务恢复正常运转。在进行灾难恢复、实施业务连续性方案时应将信息安全风险考虑在内，并且灾难响应和恢复两者应齐头并进。

建立业务弹性案例

传统安全措施仅关注防范或终止事故的发生和蔓延。当需要阻止事故的发生，或从运作失常的事故中恢复时，伴随着业务灾备策略的实施，业务连续性管理（BCM）就被提上日程。技术娴熟、经验丰富的 BCM 团队能减少企业的灾难响应时间。在事故管理和执行方面引入 BCM 的企业，也能够降低处理公司数据泄露的总成本。

努力防止网络攻击远远不够。虽然许多企业已经引入了业务连续性管理和灾难恢复方案，但旧有恢复方案（包括备份、云储存、站外归档和以及地理位置分散的冗余数据中心等要素）常常不能满足最小业务连续性的要求，更不要说处理严重的网络漏洞。

组织应对事故时，必须了解并管理业务影响和风险。考虑网络漏洞会对系统、人员和流程造成怎样的影响。即使能快速对网络漏洞做出响应，攻击产生的后果也可能蔓延。

准备好应对服务中断了么？

灾备和网络安全是团队工程。如果网络遭受近乎连续的攻击，企业系统也会面临风险。这些漏洞带来的影响受到许多因素的影响 - 其中最重要的一个因素是企业自身的准备情况。

网络安全已经不仅是 IT 部门的职责了。每个企业的业务连续性方案应当具备评估风险的拓展性协议和紧急预备方案，以便处理网络事故的潜在影响。

为了成功处理并解决网络攻击，必须充分了解公司的安全和风险态势。网络安全事故的本质核心在于数据，破坏数据完整性、可用性或数据本身会扩大网络安全事故的影响。就业务灾备而言，扩大风险评估的范围，了解其在数据层面的影响，有助于弄清楚数据破坏发生的时间、方式和数量。

业务连续性是企业为数不多的重要指标，能够从整体角度，审视组织的各个层面，从实体建筑，到技术和数据，再到员工、流程和战略。不

管结果如何，组织必须能够尽快恢复企业系统运转。

高效灾难恢复有赖于明确、灵活、周密的灾备方案，防止企业数据遭受攻击。将安全和 BCM 结合起来能高效解决事故管理和执行方面的问题，有助于应对包括网络事故和攻击在内的各种类型的威胁。

作者介绍：

Linda Laun

IBM 公司全球业务连续性及灾备服务高级技术人员

Linda Laun，IBM 首席业务连续性架构师，负责 IBM 公司 BCMS 的设计和执行，确保来自 175 个国家的 380,000 名 IBM 员工随时待命，保持工作效率，为客户提供更好的服务。她成功为全球各行各业大型或小型企业的灾备流程各个方面提供指导。2016 年，她被提名为北美业务连续性协会 (BCI) 的年度业务连续性和灾备专业人士（私营企业）。