重大疫情下的 IT 风险管理与应对

（来源：毕马威中国公众号，2020-04-07）

新型冠状病毒的疫情席卷了 2020 年的新春，也牵动了全国各方的关注，为有效抗击疫情，企业、机构、政府等组织纷纷推迟复工时间，采取远程协同办公模式，以降低集中办公所带来的疫情传播风险。

当前，远程协同办公依赖企业先进的 IT 技术，能够帮助企业在疫情期间克服困难、减少损失。而如何有效地进行 IT 风险管控，促进 IT 持续有效运转，使 IT 能够更为有效地支撑业务的持续运营显得尤为关键。毕马威结合 IT 风险管理服务方面的专业知识及实务经验，提炼出重大疫情下 IT 风险管控的关注重点及应对措施。

重大疫情下 IT 风险管控的重要关注点

1. 人员及沟通管理

在特殊期间，保证企业持续的业务运行需要 IT 的有效支持，不仅要考虑运维工作的可持续性，同样要考虑到岗人员的最小化。为应对疫情的挑战，各企业纷纷采取员工轮岗到场与远程协同办公相结合的方式，企业需考虑在此工作模式下，如何加强人员及沟通的管理，以确保 IT 运营的持续性和稳定性。

内部关键岗位的管理：

企业应梳理 IT 运营的必要工作流程，针对各工作流程识别和明确内部关键岗位；结合内部管理实际情况，对内部关键岗位安排现场人员和非现场人员、主岗和备岗的工作分配；梳理应急预案和应急联系人清单，建立及时、有效的沟通与响应机制。

IT 外包人员的管理：

部分企业采取外包人员与内部员工共同进行 IT 运营管理的模式。对于 IT 外包人员的管理，企业需要建立和完善 IT 外包应急预案，规范外包应急处理流程；定义必须在岗的外包团队人员清单，做好人员核实和管理工作；加强外包工作的定期的线上汇报与沟通，确保科技项目或运维的持续推动；开展定期评价机制，保证特殊时期 IT 外包服务质量可控。

办公及沟通模式转化：

在突发疫情的情况下，除 IT 日常运维工作外，企业也需利用数字化协同办公平台进行移动办公，从用户组织需求出发，拓宽用户办公边界，提高用户办公效率与质量；充分考虑短时间涌入的集中流量，防止协同办公平台出现长时间的卡顿，服务出现拥堵不稳定的情况。

2. 信息安全与数据安全

特殊疫情期间的远程办公模式，对于企业权限管理、敏感数据保护和网络安全防范等工作带来了重大挑战，例如，远程办公期间账号共享、临时性授权等行为可能导致关键岗位权限蔓延；敏感数据可能通过拍照、外网传输等方式泄露；网络钓鱼攻击可能乘虚而入；办公终端被迫暴露在不安全的个人网络环境下等。因此，我们建议企业结合远程办公模式的特点，在信息安全与数据安全方面加强控制和防护：

关键岗位权限的严格分离

企业应识别系统权限管理员、数据库管理员、关键业务流程审核员等操作系统层、数据层和业务层关键岗位，明确关键岗位账号的使用范围及责任归属；对于因隔离等特殊原因而暂无法工作的关键岗位账号进行回收和统一调配，禁止关键岗位账号及权限私自交由他人代管。

可将关键岗位账号与关键岗位人员设备终端进行绑定，以防止账

号共享、泄露或被窃取；记录并跟踪关键岗位账号登录的 Mac 地址，以识别异常登录。

可对关键岗位的重要操作进行身份验证，如对于重要权限操作增加手机验证码校验等。

敏感数据在办公沟通模式转化下的有效保护

启用敏感数据脱敏库，对敏感数据进行统一脱敏，并将脱敏数据、源数据、脱敏关系分别保存在不同的数据库中，将脱敏数据库向远程办公人员开放，源数据库和脱敏关系库仅后台运行，不得随意访问。

对于远程查询和调用敏感源数据，应该进行更严格的限制，如限制敏感数据的显示条数和查询次数、禁止敏感数据复制及界面截屏操作。

远程办公模式下，原则上应禁止敏感数据传输。对于特殊情况下的敏感数据传输，应采用时间戳、加密、数字证书等技术，确保敏感数据传输安全。

防范钓鱼式攻击

企业应提醒员工远程办公过程中防备热点钓鱼，不得将工作终端暴露在来历不明的 Wi-Fi 热点环境。

企业应提醒员工远程办公过程中防备邮件钓鱼，不得在电子邮件中分享系统账号、密码、银行账户等工作或个人敏感信息；对于超出正常数据收集范围的邮件请求，必须和发件人取得联系。

企业应提醒员工远程办公过程中防备链接钓鱼，对各种途径接收到的登录链接，应在点击前确认信息发送人的真实性，询问电子链接的作用、界面信息和可能收集的信息范围，或向信息安全人员征询意见。

防范网络病毒和入侵攻击

企业应提高员工安全意识，禁止员工打开或运行来历不明的电子邮件、文件及程序，禁止下载和安装非授权软件；在远程办公起始日，修改办公终端及终端内重要系统的密码，并提升密码复杂度。

企业应组织科技人员对办公终端、网络服务器的防病毒软件进行统一升级，排查防火墙配置，在有条件的情况下启用代理服务器，遏制网络病毒及网路攻击的渠道。

企业应组建专项团队加强网络监控，扩大和提高网络流量分析、安全漏洞扫描、防火墙渗透扫描等网络防护手段的范围和频率。

企业应建立应急和恢复机制，以便在遭受网络病毒或者网络入侵攻击后，降低企业损失；通过密集的数据备份策略降低数据丢失的损失等。

3.服务交付模式

当我们为火神山医院建设的中国速度而感慨激动之时，也注意到为了有效控制人员接触导致交叉感染，而在一夜之间投入使用的“无接触收银超市”，该超市实现了真正的无人化、系统化管理，而且整个建设过程只用了不到 5 小时。如何保证系统开发的质量控制是 IT 风险管理中不可忽视的一环，人员沟通、资源供给、环境控制等在疫情时期面临更多挑战的情形下，如何兼顾效率、质量与成本，也同时成为众多企业、组织和机构不得不重点关注的问题。我们总结了以下几点建议：

项目生命周期各环节人员要强化沟通，避免需求理解错位、开发进度缓慢或交付不达标等问题；同时，还需要做好投产版本控制和版本投产排期管理，确保非常时期系统投产的有序进行；

重点把控系统开发和迭代项目中的关键节点，包括计划制定、需求确认、整体方案设计、代码安全、测试验收和投产试运行，从而实

现质量和效率的双赢；

信息安全管理应贯穿始终，关注代码访问的权限管理、信息安全防护评估、客户数据保护等。

除了系统研发和投产上线，IT 运维保障支撑是确保业务连续性的重中之重。系统的运维保障服务就好似这次疫情下，一线战场人员背后全国的“后勤”支持，是维持信息系统持续、稳定、高效运行的关键。做好系统运行，确保系统在日常及特殊场景下的正常运转，我们总结了以下几方面要点：

做好 7*24 小时系统运行监控，做好容量管理工作，关注 VPN 及系统访问并发量、网络流量、内存占用率等重要关键运行指标，设定合理阈值及报警机制，为业务持续运营提供有保障的 IT 运行环境。

根据实际情况合理安排人员轮流值班，针对生产机房、数据中心等重要场所，可根据岗位分工制定值班计划，保障日常巡检工作有序进行，落实数据备份、系统作业处理等日常运维工作的有序进行。

明确非常时期事件、问题响应和处理机制，明确处理流程及应急保障措施，建立相关业务部门、科技部门内部各条线的联动机制以及运维一、二、三线的人员协同。

我们相信在多方共同努力下，我们终将战胜疫情，跨过严冬的考验，共同拥抱温暖的春天。毕马威将同企业一起努力，关注特殊时期的 IT 风险管控，为业务持续稳定运行提供有力的 IT 运行环境保障，共同应对挑战。