扫清危机上报程序中的疑问

发布日期：2020 年 1 月 30 日 - ID G00717462 -
阅读全文约需 13 分钟
企业风险管理团队项目：

风险响应策略

危机上报程序往往含糊其辞，这很容易造成危机管理计划负责人难以及时获取关键信息，进而导致反应迟缓。本研究报告旨帮助企业风险管理负责人解决这一问题。

导语

危机肇始时的应对方式将严重影响企业的危机管理效果。如果延报风险事件信息或是迟迟不采取进一步措施，企业就可能无法有效应对危机和防止重大损失。虽然很多企业都制定了标准化危机应对政策和程序来指导员工行为，但这些程序本身对如何上报处理方式含糊其辞，因而在风险事件面前往往难堪大用。

为了扫清危机上报过程中的疑问，参与危机管理的企业风险管理负责人应从场景规划转向基于影响的规划，创建简单指南以指导快速上报决策，并在危机之后进行复盘，以便更好地应对未来危机。

主要观点

- 在制定危机上报程序时，使用场景规划往往会造成很多疑问；因为这种方法无法创建精确场景，也就难以准确预测事件走向。企业风险管理 (ERM) 负责人应从危机造成的影响出发，围绕受影响的关键系统和程序进行规划，这样就无需考虑风险事件的具体情况。
- 对于负责向危机管理团队上报问题的业务领导，企业应向其提供单页指南，以便在事态上报时快速指导其相应的行动。
- 在危机之后进行复盘有助于发现待改进领域，明确未来在类似情况下应如何/何时上报风险信息。

前言

2017 年恶意软件 NotPetya 刚刚爆发时，航运业巨头马士基一开始未能准确判断情况。据当时新闻报道，马士基在几个小时后才搞清楚攻击动机，然而此时恶意软件已经造成了严重的影响，大批 IT 服务、终端用户设备、应用和服务器遭到攻击。4.9 万台笔记本被毁，1200 多种应用被锁定。

在确定事态后，马士基立刻行动起来，与可靠的外部专家共同进行了网络取证。该公司设计了一个新的 Windows 版本，检索到一个未被破坏的活动目录副本并进行了重建，同时增强了防火墙。无论是对内还是对外，马士基对此次事件都尽可能保持了透明，甚至与该恶意软件的制作者进行了对话。

虽然在本次攻击中损失超过 2.5 亿美元，但马士基的快速危机响应成功保证了业务的连续性。据马士基技术负责人介绍，在危机期间交运的货物集装箱中，95% 按时送抵目的地。此外，马士基也保住了全球最大集装箱货运公司的称号。这个例子充分体现了在危机关头快速响应的重要性。

从诺基亚和爱立信对同一危机的不同反应来看，能否针对危机快速准确的采取行动足以决定企业的命运。2000 年 3 月，皇家飞利浦电子公司位于新墨西哥州阿尔伯克基的一家手机芯片厂发生火灾，由此改变了两家电信巨头的命运。据新闻报道，车间员工发现起火冒烟后进行灭火，但由于喷头中的水是被污染的，数百万件等待交付的芯片就此报废。而这些货物分别属于两家手机巨头——诺基亚和爱立信。

一开始，飞利浦并不清楚此次起火的破坏程度，还向两家公司保证将很快解决问题，最多只需耽误一周时间。然而，诺基亚快速行动起来，直接与飞利浦的高管取得了联系，准备利用其它厂的产能。与此同时，诺基亚的工程师团队对部分手机进行了重新设计，以兼容飞利浦和其他制造商的芯片。另外一组工作人员则开始寻找新的制造商，以减小飞利浦的生产压力。

与此形成鲜明对比的是，爱立信则未着手制定任何应急方案，而是坐待该厂产能恢复。火灾发生两周后，飞利浦才不得不承认其破坏程度远超预计，车间最终关闭长达六周。至此爱立信方面已是无力回天，公司手机部门二季度运营亏损高达 2 亿美元，从此一蹶不振，将市场份额拱手让给诺基亚，自己也被索尼公司并购。而安然度过此次危机的诺基亚越发强大：2000 年 3 季度末，其在全球市场份额增长了 30%。

上面的例子凸显了危机管理方案启动决策的重要性和困难之处。从一开始来看，根本无人料到芯片缺货会演变成一场危机。火灾几周后，其破坏程度才为人所知。然而，在处理不确定性方面，诺基亚明显比爱立信技高一筹，才能尽量减小损失、甚至最终确立竞争优势。诚然，绕开不确定因素、准确判断何时启动危机管理方案并非易事，但正因为如此，它才对企业的存亡发展具有举足轻重的意义。

挑战的核心在于“何时启动危机管理方案”这一高风险问题：启动过早会造成资源浪费，还容易给人留下“狼来了”的印象，而启动太晚则会使企业不得不承担严重的财务、声誉和法律后果。员工也往往在“上报风险事件信息”与“依赖常规流程解决问题”之间陷入两难之境，前者动辄得咎，后者又常常让危机雪上加霜。不过，好在企业风险管理团队还可以通过一些可靠的方法扫除疑问。

实施基于影响的危机上报规划

在建立危机上报程序时，ERM 团队通常会瞄准某种特定风险事件的具体场景。他们认为，必须全面考虑所有可能影响风险事件的变量，才能尽可能地保证上报方案的准确性，由此针对具体危机场景提供有效的指导。遗憾的是，这样只会适得其反，造成更多不确定和降低危机管理的效果；因为我们根本无法面面俱到地预测危机事件所有可能的展开方式。

任何危机事件的发展都可能与之前的计划有所不同，结果造成无法及时上报，使得企业不得不在毫无准备地情况下面对危机。在危机处理中，时间就是一切；上报延迟会严重影响到危机减轻和恢复的效果。因此，ERM 团队不应针对具体场景构建危机管理上报程序，而应围绕危机对企业的影响来进行，避免纠结于风险事件的详细情况。风险事件信息上报之后，危机管理团队将针对受影响的领域启动预先制定的方案，包括响应和恢复措施、沟通程序和人员管理等等。同时，该团队也会针对具体变量对计划进行定制。

无论风险事件属于何种性质，危机给企业造成的影响都大同小异。例如，火灾、洪灾、地震属于截然不同的场景，然而它们可能给企业造成的关键影响基本相同：系统停机、员工缺勤、供应链中断等等。如果针对每种自然灾害都进行场景规划，那么不但需要耗费大量资源，而且由于未知因素太多，结果也不尽人意。与此相对，如果针对系统停机进行规划——而不考虑造成停机的原因——那么就会简单很多，因为它涵盖了多种危机事件。如此一来，即或危机未按照预期发展，员工也不至于手足无措。相反，一旦关键系统和流程受到某个事件的严重影响，员工就可将风险事件信息上报。为了将上报程序落实到运营中，ERM 可制定一份简单指南，针对关键影响说明正确的上报措施。

简化上报指南

企业常常利用复杂的流程图或厚重的政策手册来指导危机上报工作。然而，这些流程图和政策大多晦涩难明，执行起来也十分耗时，造成员工纠结于是否应将风险事件信息上报，结果导致响应迟缓。因此，ERM 应提供简明易行的上报指南，以帮助员工快速决策。

案例：GrayHarbor's* 上报阈值和标准指南

GrayHarbor 的 ERM 团队担心过于详尽的指南不适用于真实发生的危机事件，进而使得业务弹性管理人员——该公司负责上报风险事件信息的员工——难以快速做出决定。

为此，该团队制定了一份简单明了的指南，以帮助其做出恰当的应对。ERM 首先（根据影响量级）将事件分为三个类别，并就如何/向谁上报提供了简单说明：

- 事件——通常为能够按照具体业务部门/职能部门/工作场所现有应急响应或事件管理方案参数有效处理的紧急情况。事件不大可能升级为问题或危机，因此无需通知危机响应团队 (CRT)，只需通过定期事件汇报机制在事件解决后通知全球业务弹性 (GBR) 团队。

- 问题——通常为需要跨团队合作或启动业务连续性方案的区域性或跨部门重大紧急事件。问题可能损害企业声誉及/或在当地或业务部门内部造成严重后果，但不会危及公司的全球声誉或资产。发生问题时，应通过电话告知 GBR，并由 CRT 进行管理或提供支持。

- 危机——可能对企业造成严重损害、必须由危机管理团队 (CMT) 加以管理的情况。危机可能直接发生，也可能由事件升级演变而来。发生危机时，必须立刻通知 GBR 并由该团队激活 CMT。

然后，ERM 针对以上三种影响程度分类确定了触发点（见表 1）。

当某个标准超过阈值时，业务弹性管理人员应立刻上报。例如，如业务弹性管理人员经过评估后发现，某个事件的运营影响从单个地区扩大到多个地区，应按照危机上报程序立即告知 GBR 团队，并由该团队启动危机管理方案。

这一方法不但为该公司提供了切实可行的上报指南，也防止了过于具体的方案让业务弹性管理人员无所适从，使其得以在风险事件评估过程中做出自己的判断。

*化名。

表 1：上报标准指南

类别	事件	问题	危机
财务影响	潜在财务损失可能低于 X 百万美元。	潜在财务损失可能在 X 百万-Y.Y 千万美元之间。	潜在财务损失可能超过 Y.Y 千万美元。
运营影响	■ 本地影响——如单个场所或系统。 ■ 仅单件资产/单个场所受到影响。	■ 地区/业务受到影响。 ■ 超过一件资产/多个场所，重大资产/场所及/或多个业务部门受到影响。 ■ 影响仅限于单个地区，但实际/潜在影响可能扩大到全国。	■ 整个企业受到影响。 ■ 多件重大资产/多个场所及/或多个业务部门受到影响/潜在影响。

技术影响	■ 系统/应用停机，影响单个业务部门/场所。 ■ IT 事件例行管理流程。	■ 系统/应用停机，影响多个业务部门（如企业应用）。 ■ 网络安全事件，影响业务。 ■ 需多个业务部门发送客户通知。	■ 数据中心无法访问或多个企业系统不可用；需立即通知。 ■ 预计“问题”级别的事件造成的停机将超过 4 小时，需上报。 ■ 数据中心完全损失。
传统媒体/社交媒体报道	■ 本地市场以外的地区不大可能对此感兴趣。对公司品牌无影响。 ■ 无需企业发布声明，或在正常经营过程中发布例行/非时效性声明。	■ 感兴趣或潜在兴趣，不大可能对企业品牌造成严重损害，但可能需要立即做出反应。	■ 媒体报道可能对企业品牌造成严重损害。 ■ 需企业立即做出反应。
员工影响	■ 内部：同事受到影响，但几乎无后果。 ■ 外部：客户和患者受到影响，但几乎无后果。	■ 内部：同事受到影响，后果中等。 ■ 外部：客户和患者受到影响，后果中等。	■ 内部：同事受到影响，后果严重。 ■ 外部：客户、患者及/或社区同事受到影响，后果严重（影响程度及/或持续时间）。

健康和安全影响	受伤及/或生病，需送医院急救或现场处理。	受伤及/或生病，需紧急医疗处理；或工作场所发生与工作无关的死亡。	受伤及/或生病，需深度医疗处理；或发生死亡。
监管影响	未引起监管部门关注或仅例行关注。	监管部门发出问询；可能被报道及/或影响到经营许可。	监管部门对情况表示密切关注，及/或要求企业采取行动，及/或在计划外立即对经营许可采取措施。
股价影响	对股价无影响或在预期内。	对股价意外造成中等负面影响。	对股价意外造成严重负面影响。

来源：GrayHarbor*

危机得到控制、业务重回正常之后，企业必须对其上报程序的有效性进行评估，以确定有效措施和未来待改进领域。为此，ERM 应进行复盘。

危机上报复盘

在危机之后的恢复过程中，ERM 必须向主要利益相关方介绍事件情况，以评估响应效果。在小组环境下对流程进行评估有助于获取跨部门反馈，使 ERM 得以了解利益相关方在危机中的决策对其他相关方的影响。例如，如某业务部门领导未能及时向 CMT 上报，可能造成危机管理方案启用出现重大延迟，导致其它多个部门发生严重中断。

对于企业而言，它通过展示延迟上报的后果，强调了及时上报的重要性。此外，它也有助于发现延迟点，使 ERM 能够深入挖掘并制定行动方案，以确保未来危机能够更快地上报到 CMT，防止造成企业营收、声誉甚至生命的损失。然后，ERM 可更新完善危机上报方案，并向整个企业内部进行宣传，以体现在复盘中收获的经验教训。

结语

风险事件信息上报决策对于确保危机管理的有效性至关重要。一旦上报指南含糊其辞，就可能造成员工无法确定何时/如何上报风险事件信息，使企业为延迟付出惨痛代价。幸运的是，ERM 可通过多个步骤帮助员工清楚决策。

从基于场景的危机管理方法转向基于影响的方法，有助于简化上报决策，使员工更好地确定应当采取怎样的措施——即使危机情形与计划并不相同。基于影响的方法针对重大影响提供了上报指南，对员工而言更加明了，因为无论危机事件属于何种性质，其影响都大同小异。这样一来，就减少了员工在考虑是否上报时所必须权衡的变量。

此外，ERM 还应向负责上报的员工提供简洁明了的指南，着重强调如何正确上报具有重大影响的事件。与传统的流程图和政策手册相比，这种方法仅向员工提供与危机上报有关的最重要信息，因而有助于加快上报决策速度。最后，ERM 必须在危机之后与关键利益相关方进行复盘，以便确定上报程序中的待改进领域。利用这些方法，ERM 可大幅提高危机管理的有效性。

作者推荐

- “Crisis Management: Closing the Loop (Intuit)” ——财捷的 ERM 团队建立了一个闭环危机管理流程以有效管理危机和完善当前响应计划。ERM 负责人可采用这一方法来确保及时响应信息安全危机事件、减小企业风险敞口。
- “Crisis Communication Plan Templates” ——借鉴面向不同业务部门的危机传播计划，制定和完善贵公司的方案。
- “Crisis Communications Plan Builder” ——帮助读者把握危机管理的关键要素，并在此基础上创建量身定制的危机沟通计划。
- “Crisis Readiness Assessment Tool” ——帮助读者评估所在企业对危机的准备程度。

关于本研究报告

本研究报告基于对多家企业 ERM 负责人及其团队的采访，以及 Gartner 原创研究成果。

相关报告推荐

Manufacturing Industry Scenario 2023:Drive Innovation With Data
Forecast:Small- and Midsize-Business IT Spending, Worldwide, 2017-2023, 4Q19 Update
Peer Connect Perspectives:Who Should Product Management Report to?