基于PCR持续改进架构的情报泄密危机管理模型研究

黎小平,韦玉良

(江西财经职业学院 图书馆,江西 九江,332000)

摘　要:当前的反竞争情报领域,学者主要关心情报保护问题,而忽视情报泄密后的危机管理问题。本文基于持续性管理的思维,提出了情报泄密危机的生命周期和危机管理模型(PECR),阐述了该模型各个阶段的任务重点及相互关系。本文认为情报泄密危机的管理比情报保护往往还要重要,这项研究可为企业反竞争情报研究提供新的思路,并为企业关键性情报泄密事故的处理提供理论和实践指导。

关键字: Coombs PCR;情报泄密;危机管控;PECR 模型;BCM

中图分类号:G350　　**文献标识码:**A　　**文章编号:**1007-7634(2012)01-60-05

Study on the Model of Information Leak Crisis Management Based on Coombs´ PCR Improvement Structure

LI Xiao-ping,WEI Yu-liang

(Jiangxi Vocational College of Economics and Finance, Jiujiang 332000*,China)*

Abstracts: On the basis of the study on the theory of BCM (Business Continuity Management) and the exposition the crisis life cycle In the Coombs´PCR theory, Completed the theory migration and model transplantation and improvement, and an enterprise crisis management and control model was established, the key task of the all stages of model were expounded, which provide useful theoretical and applicable guidance for enterprises to manage the risks of business information leak crisis.

Keywords: coombs PCR;intelligence leak; crisis management and control; PECR; BCM

随着信息时代的来临,现代企业的经营者在进行战略管理特别是战略决策时会事先收集大量的宏观环境信息、市场数据、竞争对手情况等竞争情报,然后制定战略决策,以达到先于对手取得产品核心技术,或先于对手获取市场行情,或领先一步占领市场,或为产品的推广赢得先机的目的,可见,企业在运营过程中随时面临着信息泄密的风险。

实际上,对企业来说,一方面由于经济社会的发展,企业经营风险在不断增大,由于现代企业对信息技术的依赖越来越强,近年来频现的自然灾害、疫情以及企业不断面对的黑客、病毒等因素,使企业已无法完全避免信息泄密甚至信息系统瘫痪的风险;另一方面随着社会分工不断细化,企业对供应链的依赖也越来越强,企业间的合作、共存所要求的信息共享度更甚从前,信息的外散已无法完全避免[1]。然而学术界关于信息安全、竞争情报保护或反竞争情报研究较多,大多涉及是防御问题,而关于一旦发生泄密,甚至是出现泄密危机后企业如何应对问题的

收稿日期:2011-05-12

基金项目:江西省社会科学"十一五"规划(2010)重点项目(10TW04)

作者简介:黎小平(1984-),男,江西九江人,硕士,讲师,主要从事竞争情报、知识管理研究.

研究非常罕见[2]，这即是本文要探讨的内容。

1　理论基础

1.1 Coombs的PCR模型

前文提及，在如今的市场经营环境下，众多不确定的因素给企业带来了危机爆发的潜在的可能性，这导致现代企业的平均生命周期也在不断缩短，因此企业越来越重视危机管理，以便企业出现危机时能及时采取有效策略预防、控制危机及减轻其危害和损失。目前，关于危机管理的研究非常多，认识也逐渐深入。关于危机管理，著名学者库姆斯（W. T. Coombs）提出了危机管理生命周期的三阶段模型（PCR模型），把危机管理分为三个大阶段，每个大阶段中又分为若干小的阶段。

在Coombs的PCR模型中，危机的第一阶段是危机预防，该阶段任务重点是建立一套危机预警机制，包括组建危机领导小组、识别危机前兆等；第二阶段是危机处理，主要任务是采取有效措施，隔离危机，并迅速找出原因，化解危机；第三阶段是危机总结，是危机管理的最后一个环节，主要是调查危机发生的原因，并对危机预警、应对和处理等环节进行评价，并提出整改[2]。

Coombs的PCR模型中关于危机的三个阶段的描述，是危机管理的重要的基础性理论，许多学者如史蒂文·芬克、米特洛夫、若曼.R.奥古斯丁都在他的基础上提出了自己的见解，但只有Coombs的PCR模型得到了国内外大多数危机管理专家的赞同。笔者认为，该理论对于分析我们认识信息泄密危机，并提出泄密危机时的管理策略仍具有重要的指导作用。

1.2 持续性管理

持续性管理（BCM）是利用预防措施和复原控制建立的一套发展、执行、测试与维护企业应急反应计划和持续业务的管理流程，以实现保护业务流程中的关键因素，避免其因自然灾害、恶意破坏、意外事故、机密外泄等影响、中断企业业务的目的，保证企业长久稳健运营，避免股东追究责任及增强股东、客户信息，维护公司品牌和形象[4]。

BCM作为一门近年来逐渐兴起的学科，已逐渐成为国际上企业进行危机管理的通用规则，受到了学术界、企业界，特别是政府部门如此重视。从国际上看，由于那些及时引进持续性管理的企业，在面对灾难时均能化险为夷，因为企业在信息泄密等风险或灾难时，通过实施BCM，可迅速确定由此可能造成的威胁，并能提供一套架构和机制在威胁发生时采取相应策略，防止关键业务受到影响（这往往比防范危机更加重要），保障企业永久稳健运营及利益有关方的利益。所以，现在许多国家（如英国）甚至将是否制定持续性管理计划作为上市的基本条件[5]。

2　PECR：基于PCR持续改进架构的企业情报泄密危机管控模型

当企业发生情报特别是关键性情报泄密后，企业将面临巨大风险，必须启动危机管控机制，通过实施预防性和恢复性相结合的持续性管理程序，把信息泄密的后果减少到一个可接受的水平。本文参考Coombs的“PCR”理论中关于危机生命周期的描述，并进行了移植和改进，并结合BCM思想，架构了信息泄密危机发生时企业危机管控模型，这就是PECR，如图1所示。

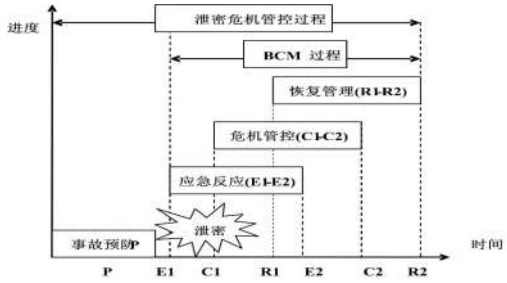

图1　PECR模型

2.1 P阶段：事故预防（Prevention）

在泄密事故预防阶段，主要任务是在分析评估可能发生泄密的风险信息点、发生事故的概率，以及建立危机管理机制，并准备危机处理过程中需支配使用的资源。

2.1.1 基础准备

事故预防首要工作是建立危机管理指挥体系（参见图2），确定管理团队、指挥官与成员。指挥官一般为高层管理人员，具有组织授权任命，对公司运营具有高层次理解。管理团队负责组织、协调、监控和领导整个指挥团队运营，该团队的设立也应符合企业政策，具有授权，并调动企业资源，以便在企业主要业务范围内实施危机管理和控制。团队可采取按业务模块分工负责，如分为风险评估小组、应急反应小组、业务恢复小组等，业务小组负责组织、指导业务模块的危机应对，是整个团队的核心。同时，考

虑到泄密事故本身的破坏性,预备好危机管理所需资源也是关键之一,如备用的服务器、线路、渠道等。备用资源可提高事故快速响应能力,最大程度减少企业损失,因而也是十分重要的。

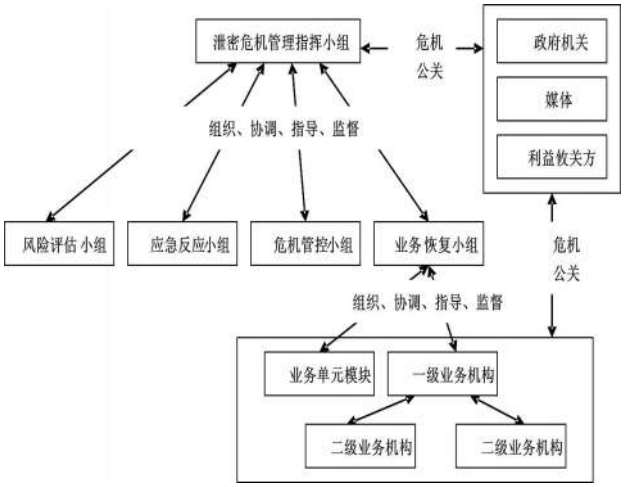

图2 泄密危机指挥体系

2.1.2 制定与维护业务持续计划

业务持续计划(BCP)的完善性是企业泄密事故快速响应处理能力的核心,其目标是帮助企业在较短的时限内识别风险点及可能会影响业务的关键性因素,阻止风险蔓延,保护业务核心。BCP应包含泄密风险点的识别、风险可能性分析、事故预兆识别、泄密损害程度分析和风险控制策略等内容[6]。除此之外,还应蕴涵成本控制思想,以便危机管理成本能小于控制威胁所能带来的收益。

⑴泄密风险点的识别、评价与分类管理。

由于现代企业非常倚赖于信息的流动与增值,企业应建立信息的分类管理与控制制度,对信息(特别是关键信息)的产生、存储、流向、流动过程、接收、销毁都要留下日志记录,同时对信息的内、外交流要严格分析与控制内容。更为关键的是,要时刻注意业务过程中可能造成泄密的业务过程或信息点,建立风险点清单,并对该风险点的运行要严格监控、记录。

目前关于风险点的识别国内外已有较多方法,企业可借鉴引用,如失效模式与影响分析
、事故树分析、危险与可操作性研究等系统性危险源鉴别方法。这些方法之间各有优缺点,可根据实际情况加以选择或联合使用。

除此之外,由于风险点发生泄密危机时所引起的预期损失程度、可能性不尽一致,它与风险点中的信息本身有关,也与诱发因素有关,可见,应对风险点进行风险评价。可建立一套风险评价模型,抽取影响危害程度的关键性因素作为指标因子,利用数据模型,以实现对风险程度的定量分析,并与定性分析等其他方法相结合,进而直接了解各信息点潜在风险的程度大小。

⑵事故预兆识别。

事故预兆是指出泄密事故发生前的异样表征或现象,它往往是细微并难以观察的。目前尚没有一套方法或体系能对这些预兆进行分析、识别与判断,因此十分依赖于专业情报人员个人的学识、经验和能力。当然这并不意味着这是个不可能完成的或仅靠个人努力完成的任务,相反,团队的思维碰撞更能出奇效。

在这一过程中,可建立环境、对手的特征库,及时捕捉、收集环境变化、竞争对手动作等现象与特征,扩大数据样本容量,分析并找出可能存在的活动规律。对出现新特征,要与数据库进行比对,识别是否存在异常,以分析可能会发生的风险或危机。

⑶业务影响分析。

业务影响分析是风险识别的深层分析,是在泄密风险评价基础上分析可能影响的业务环节、损失形式及程度等,当然这一分析是基于模拟和预测的。

业务影响分析过程实际是对企业关键作业、业务功能的系统性梳理的过程。它通过收集企业的关键作业流程,并与管理层沟通后识别可能受哪些信息的制约,哪些信息的泄密有可能会带来业务中断。分析该中断可能对公司正在进行的作业或整体财务、发展的冲击。除此之外,还应考虑的是要利用业务中断分析,组织应对策略,这主要考虑的是关键业务的备用方案,关键性资源备用是否齐全,最大允许的中断时间、恢复时间、恢复优先级等。

特别要注意的是,业务影响分析应以最差情景为依据,并分析最差情景下可能造成的损害程度,现有的BCP是否足以应对等[3]。

⑷风险控制策略。

风险控制策略是根据业务影响分析的结果所制定的解决方案,确保在发生泄密后,通过一系列的步骤、措施使企业的关键业务中的关键因素正常而持续性运转,其主要内容是如何减少损害和如何快速恢复。

①根据严重级别进行风险控制:对泄密后果严重的业务应立即中断作业,阻止危险扩大;对事故严重度较低的仍可运转,但要严密控制风险或转移风险。

②根据业务流程环节进行风险控制:对信息泄

密的各个环节分头控制，消除信息泄密造成的危险，如启用冗余资源、切断信息渠道等，特别要重视的是严格进行信息泄密源的控制。

2.2 E1–E2 阶段：应急反应(Emergency reflect)

关于应急反应的研究有较多的文献有论证，但大多数都是关于自然灾害等意外事故的，尚没有关于信息泄密后的反应与处理。信息泄密的危险与自然灾害差异很大，前者重要的是生命财产等实物安全，后者则是业务开展的虚拟安全，但这并不意味着危险程度会有轻重差别。

关于危机发生时的应急处理，主要目的是协调、整合企业内外部资源减少损失，暂不应不考虑事故后的恢复问题，其内容包括事故处理指挥体系的快速建立、标准化流程操作体系的应用。关于指挥体系前文已有论述，而在流程上目前许多约定标准和规则，比如OCAA和RECEVOR法则，笔者参照OCAA规则，建立一个信息泄密危机的应急处理流程[7]。

①了解事故对象(Objective)：迅速了解泄密发生对象、信息泄密源、信息泄密与传播范围等情况。

②分析事故状况(Condition)：根据了解的情况分析事故发生的情况，对事故的级别、危害程度、涉及的人员、业务环节等关键性因素有一个基本判断。

③确定行动方案(Action)：建立虚拟“管制区”，管制非事故处理人员进入，并根据分析结论、持续性管理计划确定行动方案、策略。

④任务指派(Assignment)：由指挥小组根据行动方案指派任务，开始实施事故处理，如隔离泄密源、停止受影响的业务、转移业务地点、转换业务人员、更改业务方案等。

当然，由于信息的价值差异很大，信息泄密的时机、环节也是不尽相同的，这导致信息泄密的危险也是有差异的。所以，只有事故危害级别到达触发点(Trigger point)才需要进行处理。

2.3 C1–C2 阶段：危机管理(Crisis management)

危机管理是应对危机的相关机制，是企业为减轻或避免危机的损害，制定和实施的一系列措施、策略。从广义上说，危机管理内涵的外延较宽泛，包括危机的规避、控制、解决、恢复及适应的动态过程。但如今许多西方教科书把危机管理称为危机沟通管理(Crisis Communication Management)[8]，这凸显了危机管理过程中的一个关键因素就是沟通，这也是本模型中的危机管理的重点所指。

良好的沟通可以使企业避免员工、债权人、公众、政府等各方的质疑，使自身在良好环境下从容应对危机。在危机管理时要明确危机的利益攸关方，并把握相应的沟通原则。若企业泄密可能会给企业造成重大损失，则可以采取以下策略：

①内部人员：对涉及到的泄密责任者要迅速、果断处理，对内部人员（如员工）以稳定、安抚为主，以自信、公开的态度进行沟通，同时实施感情攻略，保证企业人员稳定[9]。

②媒体与公众：以消解公众疑惑为主，同时主动配合媒体活动，适当利用媒体力量争取媒体支持。

③股东、债权人、合作伙伴等利益相关方：主动联系，体现诚意，及时沟通，说明情况，争取支持，重视的是维护对方的信心和保证履约的态度。

④政府机关：配合政府部门工作。

2.4 R1–R2 阶段：恢复作业(Recovery operations)

恢复作业阶段是危机处理的核心部分，该阶段的目的是使企业业务尽快恢复到正常状态。恢复作业是一项较为繁杂、困难的任务，经过重大泄密危机后，企业的业务流程、营销计划均发生了变化，企业形象、员工及市场信心尚未恢复，这将是一个漫长的重建过程。鉴于市场的二八法则，企业应着重抓住重点客户，使市场不至于快速下滑，资金周转不至于出现困难，以尽快恢复正常作业。

影响恢复阶段效能的关键因素有很多，包括资金、资源补给、损失程度、BCP的准备与执行情况、利益攸关者的支持程度等。在恢复作业过程中，识别出关键因素的不足并实时给予补足可有效提高恢复效率，使恢复工作快速完成。

在这一阶段，除恢复业务外，企业另一项重要的是任务是进行事后总结与错漏修正。

①危机总结与评估：对整个信息泄密事故进行总结和全面性的评价，包括造成泄密的原因、程度、损失大小、危机控制力度、成效、教训等各方面，总结要详实和全面。

②错漏修正：对发生泄密的漏洞要立即总结评估并反思、改正，迅速完善相关环节。

③法律声讨：这种受害型的危机重要的是需要法律的保护，世界上大多数国家均有许多的法规保

护,因此,企业应充分利用以声张权益。

④寻求机遇:危机的出现是企业重生的起点,应充分利用泄密事故重构企业流程、制度,探索运作新思路。

3 PECR模型的管理与维护

PECR模型的管理与维护是通过模拟泄密事故发生时企业现有危机管控体系运营过程来对PECR架构有效性进行评定的过程。企业通过该过程可对相关过程中的薄弱环节加以识别,并可以进行修正。该过程是一个循环迭代过程,企业通过重复性的循环检验,可实现对PECR模型的不断优化(见图3)。

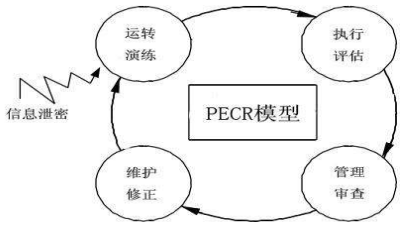

图3 PECR模型的管理与维护

3.1 运转演练(Practice)

泄密危机的演练可检验PECR模型的效用,也可提高企业成员的危机意识和危机处理能力。重复有效的演练可消除实际发生时的紧张和错误,为完善模型奠定基础。

3.2 执行评估(Do)

对于演练过程中发现的企业的容易泄密点、泄密环节、关键业务、应对策略、企业应对危机能力等各个要素进行评估,评估时可采用定性分析和数学定量模拟考核相结合的方法。

3.3 管理审查(Check)

除泄密危机外,企业面临的危机是非常多的,目前有许多专业的危机管理评估机构和标准。较成熟的危机处理规程美国FEMA的CAR EM、英国标准协会BSIPAS 56:2003等,这些规程都以BCM理论为指导,强调保护核心业务,实现企业持续性经营[4]。企业信息泄密危机作为企业危机的一种,可参考这些过程指导文件与标准建立内审机制和第三方审核机制,以实现实际运行制度与PECR模型的一致性。对审核过程通过审核表格记录,对存在的差距作为推动持续改进PECR模型的参考,以实现模型运行流程的不断完善。

3.4 维护与修正(Action)

若演练与审核过程中发现了薄弱因素,应立即由指挥小组组成团队予以研究,提出具体解决方案,以进行针对性补正,补正过程应将任务明确到个人,并作到进度追踪及限时办结,并将最后结果上报企业高层,审核通过后公布实施。

4 结 语

本文参考Coombs的PCR模型,并结合BCM思想,提出了企业情报泄密危机的管控模型,并对模型的泄密事故发生前的危机预防、基础准备阶段,事故后的应急反应阶段,事故级别达到触发点(Trigger Point)的危机管理阶段和业务恢复阶段等各阶段的任务要点进行阐释。该过程并不是一个先后过程,而应是交织融合的。PECR模型不仅是一个技术性的手段或策略组,而是一项系统性的工程。它不是静态的,而是一个动态持续改善性的模型,应通过运转演练(Practice)、执行评估(Do)、管理审查(Check)和维护与修正(Action)这一PDCA循环不断修正,以提高企业的危机管控能力。

参考文献

1 周永生.现代企业危机管理[M].上海:复旦大学出版社,2007:55-65.

2 黎小平.ISO/IEC27002:2005协议下的企业竞争情报安全管理体系的构建研究[J].图书情报工作,2011,(20):86-91.

3 Coombs W T. Ongoing Crisis Communication: Planning, Managing, and Responding[M]. Thousand Oaks, CA:Sage Publications,1999:101-104.

4 江颖俊,刘 茂.基于PDCA持续改善架构的企业业务持续管理研究[J].中国安全科学学报, 2007,(5):75-82.

5 吴海燕.论全球企业危机管理的新模式-业务持续管理(BCM)[D].吉林大学,2009.

6 刘 茜,王 高.国外企业危机管理理论研究综述[J].科学学研究,2006,24(S1):255-260.

7 雷 娜.基于项目风险和质量管理的IT服务持续性管理研究[D].北京邮电大学,2009.

8 吴启宏.论危机管理和危机沟通[J].现代管理科学,2004,(7):33-35 .

9 Vigitrust GM.Crisis management best practice-where do we start from?[J].Crisis Management,2006,(6):10-13.

(责任编辑:孙晓明)