互联网安全工程项目风险管理改进研究

王 兴,侯子文
(中国人民大学,北京 100014)

摘 要:随着计算机网络技术的快速发展,互联网的应用变得越来越广泛。网络的开放特性在带来了信息便捷的同时,也带来了个人隐私和数据被恶意侵犯或破坏的威胁。随着利润空间的减小,网络安全建设项目所涉及的不确定因素在不断增加,面临的风险及所致的损失也越来越大,因此保障网络信息的安全迫在眉睫。这就促使网络安全技术人员和实际管理人员从理论上和实践上重视对工程项目的风险管理。项目风险管理既是一门新兴的管理科学,又是项目管理的一个重要分支,更是项目经理们必备的一项与企业生命攸关的决策技术。本研究从理论框架和应对策略两个模块,对互联网安全工程项目风险管理进行了探究。

关键词:互联网;安全工程;项目风险管理
【DOI】10.12231/j.issn.1000-8772.2023.11.145

1 引言

因特网作为全世界使用范围最大的共享网络,其自身设计的开放性自由度,很大程度地方便了各类型终端计算机进行接入,充分利用了共享资源。然而因特网在早期设计时对于很多安全问题欠缺考虑,如今因特网用户发生的安全事件数不胜数,用户的自身安全受到严重威胁。从网络安全方面来考虑的话,威胁主要涉及:无授权访问、系统渗透、恶意扫描、病毒木马植入、数据窃取等。为了应对各种威胁,已有各种网络安全解决方案相继而生。随着电脑的普及和网络技术的发展,越来越多的企业选择通过网络与客户开展业务交流与合作。使用网络办理服务项目更加快捷、高效,并且企业可以在网上提供各种信息服务。但这些网络用户中不乏恶意竞争甚至故意破坏者,他们通过寻找系统内部漏洞或蓄意植入病毒、木马程序而企图潜入内部系统,从而盗取系统内部机密的数据和资料,给公司系统带来难以预测的损失。因此,网络信息安全越来越被一些企业或单位部门重视,网络安全的建设也被提上日程。而在如今环境下,网络安全建设项目所涉及的不确定因素在不断增加,面临的风险也越来越多,风险所致损失也越来越大,项目风险成为网络安全项目成功与失败的一个重要因素。这促使网络安全技术人员和实际管理人员从理论上和实践上重视对工程项目的风险管理。

2 项目风险管理的理论框架

项目指的是用来创造一种独特的产品或服务的一次性的工作内容,同时也是一种属于人类社会独特的经济和社会活动。对项目进行管理则是使用相关知识、技能、工具来满足或超过项目干系人的需求和期望。对项目进行管理不但是为了创造符合项目需求标准的产品,而且必须在项目质量、范围、时间和成本上实现项目管理目标。

存在于各个专业领域的项目内容各不相同,不同的项目有着各自的特点。而从本质上讲,项目都具有共性,无论是科学研究项目、服务项目还是建筑工程项目。项目存在的共同点可以概括如下:(1)项目组织结构的整体性。(2)项目的多目标性。(3)项目实施的一次性。(4)项目目标可确认性。(5)项目的发展性。(6)项目的临时性。(7)项目资源的有限性。(8)项目的不确定性。(9)项目的重复性。

项目的本质是一种待完成的有限任务,同时具备一定特殊性。项目也是在特定时间范围内实现单个或多个指定目标的所有相关任务和工作的集合。对于项目的定义分为三个层次:第一,是一种具备特定的环境和要求需要被完成的工作和任务。第二,需要使用有限的资源在特定的组织中于一定的时间范围内完成指定工作和任务。第三,待完成的工作和任务必须达到并符合一定技术指标。以上所介绍的三层含义也符合项目中的三种制约因素,即时间、成本和性能。然而项目的根本目标本身即为达到管理层、客户和供应商对时间、成本和性能三方面的期望。

从本质上讲,项目管理是对各种资源进行整合管理并用以实现项目目标。从根本上看,项目管理属于一种管理,具体的项目则是被管理对象。管理方法为对目标进行管理。项目团队基本都是采取临时的、灵活的以及扁平化的组织架构。工程思想贯穿了整个项目管理过程。而用于项目管理的方法论工具以及手段都比较先进和开放,需要运用多学科的知识和工具。

当科技进步迅速以及经济发展全球化,网络安全技术行业中竞争变得白热化,整体利润水平不断降低。更多的公司逐渐将侧重点向网络安全项目的风险管理倾斜,风险管理持续伴随着网络安全项目的全部过程,从项目前期预研,一直到项目的启动、执行以至项目收尾。目前

许多网络安全公司,因为项目管理人员缺乏,完全没有或刚刚开始进行网络安全项目的风险管理,更没有能力通过风险管理体系的方式来控制网络安全项目风险。经过调查研究分析,以下现象存在于国内网络安全企业在网络安全项目风险管理的工作流程中:

第一,整体项目管理意识低下和不足。目前存在的一个常见问题即项目实施和项目管理的任务无法有效辨别。导致了"无所事事"和"有任务无人做"共存的情况。通常情况下技术骨干发展成为项目经理是此问题的根本原因。其次,如果任命一个全职项目经理指定从事项目管理工作,不去做任何技术实现过程工作,例如需求分析、功能设计、代码编写、测试等,就会感觉"无所事事"或感到困惑。相对地,如果大量精力都投注于具体的技术工作,各种项目管理任务都难免会被忽视,"无人做"项目管理任务将会造成整体网络安全项目控制中出现的问题不断积累。

第二,缺少明确的预算基础。项目管理的本质是平衡进度、规格、成本和资源,然而许多国内系统集成或网络安全企业没有专业技术人员的成本结构和预算制度。所以,不能够建立实施项目的成本指标、评估和控制体系,造成企业与项目经理之间职责划分不明确。

第三,管理机制欠缺。目前,完全没有项目管理制度或仅凭个人经验进行项目管理的情况在我国网络安全企业中屡见不鲜。遵循书本制度、照搬理论,最终导致不但没有遵循实际的项目管理制度,也造成项目监理人员无法对项目实施落地过程进行跟踪指导以及支持。

第四,专业服务机构稀缺。首先,网络安全公司从整体战略角度将负责进行项目实施的模块作为系统产品销售的核心,无法定位成进行独立业务核算的组织。其次,多数采用层级化模式管理组织结构的企业,通常在经营管理和专业管理分工的组织结构方面较为欠缺。最后,垂直的技术水平程度存在组织构成上的不足。技术服务组织的市场定位被技术服务组织结构的缺陷所影响,造成其市场定位不清,未来方向不明。特别是影响技术团队的提升,导致无法长期高效地进行建设过程,并且难以增强技术团队的整体技术水平。

第五,缺少策划性。在网络安全项目启动过程对项目进行预先策划是项目经理对项目管理和控制的前提。当前项目策划方面的问题主要表现在以下几个方面:一是制订项目计划过程不合规,以至于后续执行过程中可操作程度低,导致不能严格执行计划。若项目计划太过简略,落实力度不够明确,就不能够实现任务、进度以及资源之间的平衡。二是往往不具备能够涵盖整个项目生命周期的项目工作计划,或者是采取周制的项目计划,即列出了下一周的工作计划逐周推进。三是缺乏针对项目进度全程检查和相应应对措施,无法保障项目按照预先制定的计划严格执行。

第六,项目风险意识不足。风险意识本质上是属于一种能够意识到会导致失败的因素的能力。然而现今市场环境的不够成熟和竞争规范程度不足,造成在一些系统开发项目中容易出现恶性竞争的情况。用户一般期望以较低成本来增加需求,降低价格,缩短工期。厂商则因为担心竞争出局而给出承诺,忽视了必要的科学可行性预测和分析,造成最终硬着头皮签订了无法完成交付的合同。对后续完成项目来说,还没有开始就具备了极大的风险。而风险可能带来的损失,一方面为厂商的经济和信贷损失,另一方面是给使用者也会带来经济或者生产效能的损失。

第七,实际使用人员缺乏项目参与意识。很多时候,只有一些技术人员参与系统开发。这种情况的原因常常是企业对网络安全的认知为完全属于信息安全部门的事情,而业务部门工作繁忙,无法抽出时间或精力参与网络安全项目。然而业务部门对网络安全的要求较高,从而经常性地更改需求。虽然这些理由并非不合理,不过究其根源,网络安全项目最初是来源业务部门的,项目完成后也会交付并配合业务岗位人员使用。

通常情况下,采用项目管理体系进行管理的项目对象都具有技术复杂度高、工作量大、不确定性多的特点,在管理方式方法上针对不同项目的特点需要进行有针对性的处理。

从项目过程的角度来分析,项目过程中遇到的风险是必然存在的,同时也是整个项目管理过程中不可分割的一部分。与其相关的因素很多,在许多系统工程管理技术方面也十分适用。一般来讲,对风险管理的定义有三种:(1)风险管理是为系统识别和评估风险因素而进行的标准化过程。(2)风险管理是一种正式的、系统的方法,用于评估可能引起不必要变化的影响范围。(3)风险管理是一种决策艺术与科学在管理协调、风险预测和应对方法制定等方面的融合。总而言之,对项目进行风险管理即指项目团队对项目中可能遇到的风险进行整体预测、计划、建立应对措施和项目监控的过程,本质上属于一种通过科学手段方式实现最大可能保障项目的安全。

3 网络安全项目的风险应对

3.1 网络安全项目风险应对策略

在网络安全项目中,为了规避风险,一般可以从三个方面提出策略:改变风险后果的性质、控制风险发生的概率或风险后果的大小。从结合风险产生的具体动作类型看,与其他项目又略有不同,基本可以分为以下六类:

(1)降低风险。主要通过预期来降低风险,减轻风险的负面后果,从而达到降低风险的效果。一般在网络安全项目中都会针对较容易出现或严重的问题制定应急预案。比如某零部件接入的网络安全设备导致了网络中断,排查具体的原因会消耗一定的时间,也就是业务中断成本。如果业务中断成本大于失去该网络安全设备的防护

效果所带来的安全风险成本时，那么将该网络安全设备下线处理相对于排查具体的问题原因是一种减轻手段。

(2)风险防范。作为一种积极的风险应对策略,风险防范一般采用以下两种方法:第一,无形方法。网络安全项目经理和其他项目成员的不当行为都可能构成项目的风险因素,而在实际网络安全项目中,经常出现项目成员对网络安全风险理解浅薄的情况。因此,为了减少不当行为带来的风险，必须对项目相关人员进行网络安全风险意识和风险管理教育，提升项目组整体的网络安全风险意识。第二,有形方法。工程方法是一种有形的手段,这种方法是利用工程技术来消除物质风险的威胁，也就是采取直接手段处理风险的方法。比如在对系统进行安全补丁升级或配置加固前，为避免升级补丁或配置加固后造成系统服务无法恢复的异常,提前对系统进行备份,一旦出现问题即进行恢复或回退。

(3)规避风险。风险规避是指一种策略,用于在项目威胁的可能性高,同时不利后果不是很严重,也没有其他可采用的策略时，主动放弃项目或改变项目目标和行动计划的一种风险应对策略。在一些安全加固服务项目中,出现实际加固内容可能与现有业务系统产生兼容性冲突的风险时，可以考虑放弃做安全加固的目标改为通过网络安全设备在网络中进行安全防护。

(4)风险转移。风险转移是指将风险转移给参与同一项目的其他人或组织，因此也可称为分担风险的伙伴关系。一般在网络安全项目中,由于相应匹配的技术人力资源往往并不丰富，因此采用此类动作的情况以人力资源风险情况较多。

(5)接受风险。接受风险也属于一种风险应对策略,指的是愿意承担项目风险带来的后果。一般应用于采取其他策略手段的成本高于风险带来的损失的情况。例如在上文规避风险中提到的场景中，如果采购安全设备的成本高于预算，且关联的兼容性冲突风险的系统并不重要且存在的漏洞不易被利用时,可考虑接受风险。

(6)风险储备。网络安全项目中,往往涉及较多的角色,特别是在技术方面,经常会遇到出现应急风险情况时需要协调多角色协作的情况。为了缩短风险处理响应和处理时间,为了给各相关方提供有效的协调和合作机制,结合具体的网络安全项目风险产生的规律提前编制应急措施或应急预案,并建立科学有效的项目风险计划。当项目的实际进展情况与预期不符时，就应采取既定应急措施,启动风险储备。

3.2 网络安全项目风险应对技巧

由于网络安全项目风险存在复杂性和可变性，这两种特性将显著提高项目风险应对的要求。比起其他类型项目风险的处理方法，在处理网络安全项目风险时需要更多的创造能力和协作能力。(1)创造能力。创造能力即是原创思想的本质，在应对网络安全项目风险时要求项目成员具有一定的创新思维模式,灵活思考,找寻处理风险的最佳方案。(2)协作能力。是指两个或多个具有互补技术能力的项目成员个体相互影响并达成共识，以充分发挥团队能力。比如一个项目组成员有网络方面技术专长,而另一名项目成员则有系统方面技术专长,而项目对这两方面技术都有较高要求时，即需要发挥协作能力共同完成项目目标。

3.3 网络安全项目风险的应对措施

项目风险管理是在对网络安全项目的成功构成威胁之前,对风险源进行识别、处理和消除的过程。控制和管理项目过程中的风险，能够在很大程度提高整体项目的成功率。一般来说,网络安全项目风险可以采取以下几种应对措施:(1)风险缓解:应事先确定风险发生后的补救缓解方法并在风险发生时采取对应的动作。(2) 危机处理:应对模式一般为救火模式,只有在风险造成影响后才进行应对。(3)失败处理:感知风险并快速进行反应,不过只有在发生风险之后才做出反应。(4)消除风险根源:主动清查并清除可能引发风险的苗头。(5)风险预防:计划并实施风险识别和风险防范是网络安全项目重要的一部分。

4 结束语

由于网络安全的特殊性、重要性以及复杂性,在网络安全项目过程中需求设计可行性分析和设计方案验证过程,必须着重加强对项目风险的分析。预测可能对网络安全项目整体进度或质量产生影响的风险，采取合理的应对措施消除这些风险,是网络安全项目经理的核心目标。在网络安全项目管理过程中，网络安全项目经理必须采用适用于自身风险管理的风险管理方法，以实现网络安全项目在合理的预算以及期限范围内完成交付，同时达到项目的质量要求。

参考文献

[1]谢小杰,王猛,杨刚,等.探讨企业科技项目管理问题与优化创新[C].中国电力设备管理协会第二届第一次会员代表大会论文集,2022:110-112.

[2]曾令东,董鹏,刘刚.某信息化系统工程项目进度管理研究[J].项目管理技术,2022,20(05):66-70.

[3]孙利民,潘志文,吕世超,等.智能制造场景下工业互联网安全风险与对策[J].信息通信技术与政策,2021(08).

作者简介:王兴(1987-),男,汉族,山西吕梁人,本科,初级经济师,研究方向:银行风险管理;侯子文(1990-),男,汉族,甘肃天水人,本科,职员,研究方向:数据管理。