学校编码：10384　　分类号_____密级_____

学号：17520131151207　　UDC_____

厦门大学

硕　士　学　位　论　文

企业网络风险内部控制：基于 COSO 2015 白皮书的研究

The Internal Control of Enterprise Cyber Risk: Based on the Research of the COSO 2015 White Paper

周洁

指导教师姓名：陈汉文教授

专　业　名　称：MPAcc

论文提交日期：2016 年 4 月 15 日

论文答辩时间：

学位授予日期：

答辩委员会主席：_____

评　　阅　　人：_____

2016 年 04 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果,均在文中以适当方式明确标明,并符合法律规范和《厦门大学研究生学术活动规范(试行)》。

另外,该学位论文为(　　)课题(组)的研究成果,获得(　　)课题(组)经费或实验室的资助,在(　　)实验室完成。(请在以上括号内填写课题或课题组负责人或实验室名称,未有此项声明内容的,可以不作特别声明。)

声明人(签名):

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

互联网让信息共享成为现实，并深入影响着人们的生活。但随着公司核心技术被窃取、重要客户信息被盗以致客户流失等事件的屡屡发生，它的弊端引起所有企业的思考和重视。在利用好信息共享优势的同时，如何保障自己企业的重要信息安全，减少网络恶性攻击，对于所有企业均至关重要。这不仅仅要求企业网络防御技术的提高，更重要的是网络信息安全措施能有效执行。在此背景下，美国 COSO 委员会于 2015 年 1 月发布了《网络时代的内部控制》。该白皮书提出，对任何一个企业而言，网络风险是不可能避免的，只能对其进行管理，使得企业处于一种安全、警惕、可恢复性强的状态。该白皮书实质上是利用 COSO2013 年内部控制整体框架来阐述了内部控制是如何帮助企业管理网络风险和实施控制，为企业在信息时代应用该框架管理网络风险带来了具体应用的指导性思路。

目前，我国财政部会计司联合德勤（中国）翻译了该文，但并未提出适合我国的建议。针对企业网络风险管理，我国在颁布的相关指引中略有提及。相关学者在研究、借鉴的基础上提出建议试图来帮助企业进行网络风险管理，但是因为其成果的框架性、高度专业性和行业针对性，实践水平不高，很多先进的方法都还停留在理论研究阶段，真正运用到企业的情况仍旧不容乐观。

基于此，本文首先分析了网络风险对企业的严重威胁，梳理了国际上现有的相关框架标准后，认为通过内部控制来进行网络风险管理存在必要性。然后，系统介绍了 COSO2015 白皮书中的企业网络风险内部控制基本思路，并分析了该思路的创新点。最后，通过分析我国企业网络风险管理的现状，对比我国现有的内部控制相关指引，为我国完善内部控制体系建设提出建议。同时，也针对我国企业的特性，强调企业必须认识到网络风险的不可避免，提倡企业以控制环境和监督活动为基础，通过良好的风险评估、控制活动和信息沟通机制来管理网络风险，构建一个安全、警惕和可恢复性强的企业。

关键词：网络风险；内部控制；应用研究

Abstract

The Internet allows Information Sharing to become a reality, and deeply affects people's lives. However, with the stolen of enterprise's core technology and important customer information which caused the customer churn occurring frequently, the disadvantages of the Internet have attracted all the enterprise's attention and reflection. In the use of the advantages of Information Sharing, at the same time, how to safeguard their own important information security and reduce the vicious cyber-attacks, are vital for all the enterprise. This not only requires the improvements of cyber defense technology, more important is the information security measures can be effectively executed. Based on this background, COSO issued *COSO in the Cyber Age* in Jan 2015. The white paper puts forward that the cyber risk of any enterprise is not something which can be avoided. Instead, it must be managed to make the enterprise secure, vigilant and resilient. This white paper substantially leverages the 2013 Internal Control-Integrated Framework to demonstrate how COSO can help manage cyber risks and controls. It brings a specific guiding idea for the enterprise application of this framework to manage cyber risks in the Information Age.

At present, Ministry of Finance Accounting Division and Deloitte (China) have translated this paper cooperatively, but did not put forward any recommendations for our country. As for the enterprise cyber risk management, the Chinese government briefly mentioned in some relevant guidelines promulgated. Related scholars have made some recommendations on the basis of research to attempt to help enterprise carry out the cyber risk management. But because of highly-professional and industry-specific, many advanced methods are still in the phase of theoretical research, and the situation of the enterprise truly applied is still not optimistic.

Based on the above, this article analyzes the serious threat caused by cyber risks to the enterprise, combs the relevant existing framework and international standards, and points out that the internal control of enterprise cyber risk have existed its necessity. Then, this article systematically introduces the basic idea of the internal

control of enterprise cyber risk in the white paper issued by COSO in 2015,and analyzes its innovations. Finally, by analyzing the current situation of the enterprise cyber risk management, and comparing with our existing internal control guidelines, this article puts forward the proposal to perfect the internal control system construction of our country. At the same time, according to the characteristics of Chinese enterprise, this article emphasizes that the enterprise must realize the unavoidability of cyber risks, advocates to build a secure, vigilant and resilient enterprise through the good risk assessment, control activities and information &communication based on the control environment and monitoring activities.

Keywords: Cyber risks； Internal Control； Applied research

目录

Contents

第一章 绪论

1.1 研究背景及研究框架

纵观当下，全球正在经历着以互联网信息技术为核心的第三次技术革命（刘嘉欢,2015[1]），这些新技术从根本上推动着全球的社会发展和经济增长，让我们告别了工业时代，并正式进入信息时代。自从 1989 年互联网的出现，一个全新的网络经济自此拉开了迅猛发展的序幕。互联网让信息共享成为现实，并潜移默化地影响着我们的生活，成为日常的必需品。基于此，在互联网构建的全新社会生活形态下，企业实现了全方位的动态和高效集中管理（罗敏,2011[2]），可见互联网对企业发展的影响愈发呈现举足轻重的地位。但是，随着一桩又一桩网络信息泄露事件，如公司核心技术被窃取、重要客户信息被盗以致客户流失等类似事件的屡屡发生，它的弊端却愈加明显地展现在公众面前，不得不引起所有企业的思考和重视。在这样的时代大背景下，互联网一方面成为企业运营和管理不可或缺的工具，另一方面带来的新风险也成为了企业管理和内部控制的重要对象（石爱中,2006[3]）。经营活动形式的转变造就了管理活动的相应变化（汪海青,2014[4]），对于所有企业而言，在利用好信息共享优势的同时，如何保障自己企业的重要信息安全，尽量减少网络恶性攻击，其重要性不言而喻。这就不仅仅要求企业网络防御技术的提高，更重要的是要保证网络信息安全措施的有效执行以适应时代的发展。

在此背景下，美国 COSO 委员会于 2015 年 1 月发布了《网络时代的内部控制》（COSO in the Cyber Age），该白皮书以信息技术改变商业运营为背景环境，指出每一次技术进步都伴随着风险和代价，而信息技术的发展势不可挡。因此，该白皮书认为，对于任何一个企业而言，网络风险是不可能避免的，只能对其进行管理，并致力于让企业处于一种安全、警惕、可恢复性强的状态（Mary 等,2015[5]）。要实现这样的目标，管理层就应该通过识别企业最重要的目标，执行合理成本的安全控制来保护该企业最重要的资产。该白皮书实质上是利用 COSO2013 内部控制整体框架来阐述内部控制是如何帮助企业管理网络风险和实施控制的，为企业在信息时代应用该框架管理网络风险带来了具体应用的指导

性思路。

我国对于信息技术的理论研究相较于国外起步晚，但是对于信息技术成熟产品的应用和普及程度却毫不逊色。在对互联网络运用的方面，根据 2016 年 1 月中国互联网络信息中心（CNNIC）发布的第 37 次《中国互联网络发展状况统计报告》显示，“截止至 2015 年 12 月，我国网民规模达 6.88 亿人，其中手机网民为 6.2 亿人，占总规模的 90%以上，互联网络普及规模达 50.3%，说明达半数的国人已经成为了互联网的弄潮儿，2015 年我国新增网民 3951 万人，增长率为 6.1%，相较于 2014 年提高了 1.1 个百分点。”[7]伴随国内互联网超速发展而来的，同样是诸如信息曝光等网络风险带来的负面影响，甚至让有的企业深受其害，因此，进行网络风险的管理，对于我国所有企业而言，同样均具有实用性和迫切性。

在我国颁布的像《企业内部控制应用指引第 18 号——信息系统》、《商业银行信息科技风险管理指引》等一系列的指引中，有对网络风险的管理提出一些建议和要求，相关的学者们也进行了学术研究和借鉴并提出了相关建议来帮助和引导企业进行网络风险管理，但是因为这些成果的框架性、高度专业性和行业针对性，其实践性水平不高，很多先进的方法都还停留在理论阶段，真正广泛运用到企业中进行网络风险管理的情况仍旧不容乐观，就连华为这种以信息技术为核心的大型跨国企业都难逃网络袭击的魔爪，更何况其他的企业呢？而且，虽然在美国 COSO 委员会授权下，我国财政部会计司联合德勤（中国）翻译了上文提及的该白皮书，并予以刊发，希望为我国企业建立内部控制机制以适应当下网络环境并保障网络防御体系的有效实施提供参考借鉴（Mary 等,2015[5]），但是，并未结合我国的具体情况加以建议，而只是直接翻译。

因此，鉴于 COSO 颁布的该白皮书具体阐述了内部控制整体框架如何帮助企业进行网络风险管理，对那些已经建立起内部控制的公司迅速明确如何通过有效的内部控制来设计、建立和执行网络风险管理的标准和措施，具有十分重要的指导性意义。而且更重要的是，我国企业也同样面临着严重的网络风险威胁，因此，本文将以借鉴 COSO《网络风险的内部控制》中提到的企业网络风险内部控制基本思路为基础，按以下研究框架对我国如何进行网络风险的内部控制制度建设和企业实践应用进行分析研究：

首先，通过相关权威机构的统计数据和美国医保公司 Anthem 的网络袭击案

来分析了网络风险对企业产生的严重威胁，认为网络风险已经成为企业最主要的风险之一，并将在未来持续影响着企业。梳理国际上现有的关于企业网络风险管理框架和标准，认为相关框架依赖较高水平的公司信息技术和较完善的内部治理结构，而极其专业化的标准与公司管理之间又缺乏一座沟通桥梁，以保证它们能够有效执行，因此，网络风险内部控制有其存在的必要性。

然后，回顾了 COSO2013 内部控制整体框架的演变和具体内容，并在此基础上系统介绍了《网络风险的内部控制》中基于 COSO2013 内部控制整体框架的企业网络风险内部控制基本思路，并据此分析了它相较于其他网络风险管理框架和标准的创新点。

最后，通过对我国企业网络风险管理的现状进行分析介绍，并将基于 COSO 框架的网络风险内部控制基本思路与我国现有的内部控制相关指引对比，一方面为我国在信息时代构建最新的内部控制指引提出建议，另一方面也针对我国企业的特性，提出企业在信息时代，必须认识到网络风险的不可避免性，强调在企业内部建立完善内部控制的重要性，提倡企业以控制环境和监督活动为基础，通过良好的风险评估、控制活动和信息沟通机制来管理网络风险，构建一个安全、警惕和可恢复性强的企业。

1.2 我国对网络风险管理的研究

1.2.1 法律法规

目前，作为全球最大的网络市场，2014 年 2 月 27 日，我国中央网络安全和信息化领导小组成立，可见国家对于网络风险和信息安全的重视。但我国在网络安全方面的投入占比仅为整个信息系统比重的 2%左右，仍远低于欧美国家 10%左右的水平[8]。不仅如此，从 1994 年起，我国虽然已经出台了许多互联网相关的法律法规，但大多也都是以规范整个网络环境为目标，其中针对公司内部管理层面的指引又很少和太过粗略，对身处日新月异网络环境中的企业而言，可以参考用来进行自己公司网络风险管理的指导意见和管理指引，可谓杯水车薪。

（1）规范互联网环境的相关决定

1994 年 2 月 18 日由国务院颁布的《中华人民共和国计算机信息系统安全保

护条例》，填补了我国互联网方面法律的空白。1994 年，我国的互联网建设才刚刚起步，应用程度远不如现在，因此，该条例的颁布主要是为了保护计算机信息系统的安全，促进计算机的应用和发展。鉴于当时互联网发展的局限性，网络风险影响范围较小，可控制力也很强，因此，该条例主要从安全保护、安全监督和相关的法律责任方面着手，对在发现信息安全隐患时各部门的行动和职责划分进行了明确的规定，要求由国家公安部主要来进行管理，并在总则中首次提出“任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全” [9]，如果有危害行为的，将会对其追究民事责任，强调了对网络风险肇事者的坚决处理态度，为未来我国规范化的互联网建设奠定了良好的基础。

2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过了《全国人民代表大会常务委员会关于维护互联网安全的决定》，并于 2011 年 1 月 8 日根据《国务院关于废止和修改部分行政法规的决定》对此进行修订。该决定的出台主要是考虑到互联网已经在我国的各项事业建设中得到广泛应用，对广大群众已经开始并将继续发生深刻的变化，对于加快我国市场经济的建设、科学技术的发展和社会服务信息化进程的推动具有重要作用。该决定不仅仅是为了保障互联网的安全运行，更主要的是对破坏国家安全和社会稳定以及扰乱社会主义市场经济秩序和社会管理秩序的行为进行了较为详尽的界定，并且由以前的民事责任，升级为对破坏信息安全构成网络违法犯罪行为的要依法追究刑事责任[10]。这一方面说明了，国家对互联网监管的力度越来越大，另一方面也说明了，在短短的六年间，我国的互联网发展可谓迅猛如虎，并且将在未来很长一段时间推动着国家的发展，因此，必须在强有力的法律保障下，才能更快更好地实现创造它的初衷，造福人民。

国家对于互联网健康环境管理的脚步并未就此停滞，2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过了《全国人民代表大会常务委员会关于加强网络信息保护的决定》，该决定更全面细致地规范了网络行为，保障网络信息安全。其中，第四条要求“网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的

情况时，应当立即采取补救措施。”[11]

（2）管理网络风险的相关指引

不仅仅是互联网大环境的条例和决定，国家有关部门也意识到了网络风险给各行各业带来的挑战，因此，在其出台的部分指引中对网络风险、信息安全等方面进行了简要的规范。

2006 年 6 月 6 日，国务院国有资产监督管理委员会以通知的形式，印发了《中央企业全面风险管理指引》。该指引主要是针对国资委履行出资责任的企业，希望通过内部控制系统进行全面风险管理以应对企业风险，实现企业风险管理目标。该指引强调了信息搜集的基础性和重要性，认为要进行风险管理就应该根据不同的风险管理目标来搜集信息，并将风险划分为运营风险、战略风险、市场风险、财务风险、法律风险等[12]。其中，在营运风险下就提到了关于网络风险的信息，要求企业进行网络风险管理，应该对“信息安全管理中曾发生或易发生失误的业务环节或流程”加以重视，对“现有信息系统操作运营情况进行监督、运行进行评价，并持续改进”[12]，并认为通过合理的内控方案，保持经营战略与风险策略一致，才是最佳的风险管理途径。

2009 年 6 月 1 日由中国银监会颁布的《商业银行信息科技风险管理指引》，该指引适用于特定行业暨国内的法人商业银行，突出强调了信息技术与银行业务发展的深入融合性，弥补了银行业缺失信息系统控制规范的空白。该指引从控制环境、控制活动、信息安全和系统开发、运营和维护[13]等方面，为商业银行建立较好的信息系统控制机制提供了参考，极大地提高了商业银行的内部控制效率。该指引认为“信息科技风险，是指信息科技在商业银行运用过程中，由于自然因素、人为因素、技术漏洞和管理缺陷产生的操作、法律和声誉等风险。”[13]而技术漏洞是最容易造成信息泄露的情况，并在指引的第三章指出应该从“物理安全”和“人员安全” 两方面来保障银行信息的安全，对于信息科技的外包也应该定期进行风险评估。同时还应该重视全在风险区域，通过审批、授权、验证和调节等手段来检查、平衡以及控制风险。

2010 年 4 月 15 日由国家财政部颁布的《企业内部控制应用指引第 18 号——信息系统》基于将企业内部控制转化为信息化管理平台的形式，来提高企业管理能力的背景，从企业信息系统的开发和运营维护两方面，来为企业将内部控制信

息化提供指引。因为作为企业治理的核心，内部控制系统涉及企业的方方面面，将其信息化为一个信息系统，如果无法保障它的安全性、保密性和可靠性，那么对于企业来说可谓得不偿失。因此，该指引中明确指出在网络时代，该信息系统有可能因为“系统运行维护和安全措施不到位”导致信息泄露给企业带来巨大损失，认为“企业不仅仅应该通过安装安全性能较高的软件来防范网络恶意攻击，还应当根据业务性质、重要性程度、涉密情况等确定信息系统的安全等级，建立不同等级信息的授权使用制度，采用相应技术手段保证信息系统运行安全有序”[14]，并建立信息系统安全保密和泄密责任追究制度，在与第三方专业机构合作进行业务外包时，应签订相应的保密协议，以巩固诚信可靠的合作关系，防止公司信息外泄。

2012 年 7 月 10 日中国人民银行为加强金融行业信息安全管理和技术风险防范，保障金融行业的信息安全，出台了金融行业信息系统信息安全等级保护系列标准。该系列标准为首次发布，具有具体化、行业化的特点，利于金融企业的参考和应用，其中包括《金融行业信息系统信息安全等级保护实施指引》（JR/T0071-2012）、《金融行业信息系统信息安全等级保护测评指南》（JR/T0072-2012）、《金融行业信息安全等级保护测评服务安全指引》（JR/T0073-2012）三项标准。实施指引主要从安全技术和管理两个方面确定了对不同等级信息系统的要求[15]；测评指南则是对实施指引中的测评提出了具体的方法，对实施指引起到完善和补充的作用[16]；安全指引则是在参考国家、国内相关标准之后，对机构安全、人员安全、过程安全、测评对象安全、工具安全等方面提出的具体要求[17]。该系列标准中的指引和指南，在相互补充、相互融汇后，更便于金融企业对内部信息系统安全等级的划分，也利于金融企业网络风险的识别和管理。

随着互联网越来越深入人心，很多的企业也看到了利用互联网来进行商业拓展的机会。“互联网+”已经成为家喻户晓的新名词，它的低门槛和广范围，让很多企业受益匪浅，金融行业自然也是不甘落后。再加之去年尤为火爆的股市，互联网金融更是炒作得红出了新境界。在此背景下，为了鼓励创新、规范市场、保障公众利益，2015 年 7 月 18 日人民银行、工业和信息化部、公安部、财政部、国家工商总局、国务院法制办、中国银行业监督管理委员会、中国证券监督管理