KPMG

统筹协调 主动监管：
董事会之网络安全监管之道

kpmg.com

统筹协调 主动监管：
董事会之网络安全监管之道

网络攻击和数据泄露是全球企业面临的常规风险，预示着企业随时可能成为下一个攻击目标。法律界正在深入探讨公司董事会因未有效履行网络监督职责而承担的责任以及潜在风险[1]。投资者和监管机构也日益施压，要求董事会网络监督工作，增加违规事项的透明度，披露违规事项对企业的影响。

在这种背景下，董事会和审计委员会已经逐步意识到网络安全风险应作为公司管理的重中之重。毕马威2015年风险管理调查显示[2]，中国内地和香港有近40%的高管将技术和网络安全（包括信息安全和数据隐私）列为行业五大威胁之一。如今，审计委员会面临的关键问题是：企业应获取哪些信息才能确认管理层正在有效应对网络风险？显然，要回答这一问题，董事会应首先听取首席安全官或首席信息官的意见，他们是该领域的专家，可以协助董事会从风险治理视角分析和把握总体网络风险形势。基于此，董事会应首先关注哪些方面？

我们发现，董事会经常思索：我提的问题正确吗？怎样才能确保方案成功？采取的措施充分吗？怎样才能知晓所做的事是否正确？我们的决策正确吗？

网络安全：企业和董事会的当务之急

2015年，国家互联网应急中心（CNCERT/CC）公布的报告显示，2014年CNCERT/CC共成功处理各类网络安全事件的总数为56072起，较2013年的总数31180起增长79.8%，针对互联网尤其是移动互联网恶意程序日益猖獗的发展趋势[3]。

目前，公司董事会已意识到网络安全管理工作的急迫性和重要性，因为这已不是简单的信息技术问题。事实上，网络风险已成为关乎整个企业的重要风险管理事项。

2015年6月，第十二届全国人大常委会第十五次会议审议通过《中华人民共和国网络安全法（草案）》[4]，其中要求企业的经营者提升对网络安全风险管理的重视程度。*“建设、运营网络或者通过网络提供服务，应当依照法律、法规的规定和国家标准、行业标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范违法犯罪活动，维护网络数据的完整性、保密性和可用性。”*

[1] “The Morning Risk Report: Cybersecurity Responsibility Falling to Boards,” 风险合规期刊，华尔街日报，2015年3月4日，http://blogs.wsj.com/riskandcompliance/2015/03/04/ the-morning-risk-report-cybersecurity-responsibility-falling-to-boards/.

[2] “Risk Management: Looking at the new normal in Hong Kong”，毕马威，2015年9月10日，http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Pages/RM-looking-at-the-new-normal-in-HK-201510.aspx.

[3] “2014年中国互联网网络安全报告”，国家互联网应急中心，2015年6月2日，http://www.cert.org.cn/publish/main/upload/File/2014%20Annual%20Report.pdf.

[4] “中华人民共和国网络安全法（草案）”，第十二届全国人大常委会第十五次会议新闻稿，2015年6月，http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm

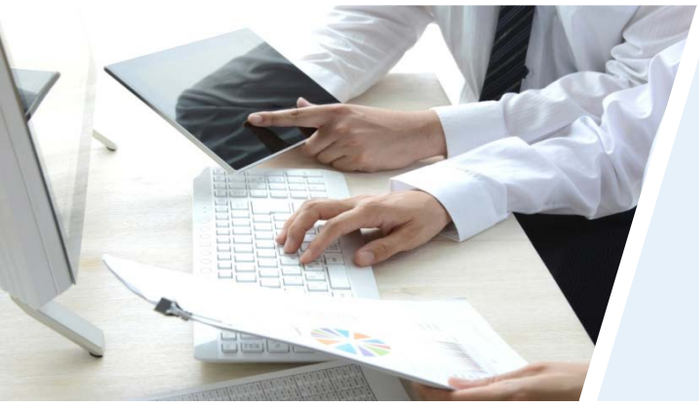
我们认为，网络安全并非难以管控，关键是公司要协调信息技术与业务部门，积极主动地加强网络安全治理，向董事会提供必要的信息，有针对性地解决网络安全威胁以及重大违规产生的不利影响。

濒于险境

近年，随着跨国企业相继成为网络犯罪的目标，董事会加强网络安全监督已不再是少数企业的较佳实践，而是所有企业都应该面临的必然选择。投资者、政府和国际监管机构日益要求董事会加强对该领域的监督力度，同时，监管机构还要求保护个人信息，并确保各系统在发生数据泄露和蓄意攻击后能够迅速恢复运行。

网络风险可导致以下后果：

- **知识产权损失：**包括专利信息、商标注册的材料、客户名单及商业敏感数据
- **法律费用：**包括数据隐私泄露引发的损害赔偿、延期补偿、监管罚款、辩护费用等
- **财产损失：**交易信息延迟提交或未提交失败
- **信誉损失：**市场价值下降和商誉损失，使客户和供应商对企业失去信心
- **时间损失：**投入时间调查事件原因及丢失的信息（如有），需持续向股东和监管机构进行解释和说明
- **管理费用：**用于缓解不利影响，例如修复客户信心，与监管机构沟通，更换财产，恢复业务水平等



网络安全治理计划实施方案

由于企业情况各异，因此治理计划也不尽相同。在网络安全治理方面，有的公司治理能力尚未成熟；有的虽已开始应对网络犯罪，但管理要求比较空泛；还有一些公司已制定实施较完善的治理计划，但仍有改进余地。

不论处于哪一阶段，有一点是明确的，那就是企业对于网络安全治理一定要未雨绸缪，不能把网络安全治理简单视为信息技术工具。打击网络犯罪需要公司上下共同努力，制定实施有效的计划和流程。在治理过程中，有些因素要随着环境变化不间断地加以考虑。

董事会的职责变化

最近一项网络安全调查显示[5]，在约1,000名IT和IT安全高管人员中，仅有22%表示企业的安全主管需要向董事会简要汇报网络安全战略。66%的人预测，未来3年内安全主管将定期向董事会通报网络安全状况。此外，仅有14%的人表示，企业的安全主管直接向行政总裁汇报工作。30%的人预测，未来三年内安全主管将直接对行政总裁负责。[6]

在确定董事会的角色时应考虑以下因素：

- 高级管理层和董事会在管理、监督网络安全和应对网络事件中分别担任什么角色？谁承担主要责任？
- 企业是否有信息安全总监？向谁汇报？是否直接向行政总裁汇报？
- 是否需要专门成立网络风险委员会，以加强定期沟通？

沟通频率

近期，美国公司董事协会（NACD）[7]对上市公司1,000余名董事进行调查，结果有一半以上（52.1%）的董事认为管理层没有提供足够的网络安全和信息技术风险信息。

关于沟通频率，应考虑以下事项：

- 是否有定期会议？频率是否足够？
- 能否定期指导？频率是否足够？
- 与管理层能否定期沟通？频率是否足够？管理层多久接收一次报告？

沟通的有效性

此外，美国公司董事协会调查发现，有35.5%的人对网络安全和IT风险的信息质量表示不满，这一比例较上年有所上升[8]。

关于沟通的有效性，应考虑以下事项：

- 企业是否制定了全面机制，确保在整个企业内实现高效、快速的沟通？
- 提出的问题是否“正确”，分享的信息是否“正确”，能否确保得到可靠的信息流？
- 管理层组织的会议、指导和沟通，其效果和质量如何？
- 企业接收的报告质量如何？是否对利益相关方保持透明度，并提供了必要的信息？

[5] “2015 Global Megatrends in Cybersecurity”，p. 3, 由Raytheon和Ponemon institute赞助，2015年2月，http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf.

[6] Ibid., p.4.

[7] “Board members unhappy with information on IT, cyber security,” 美国公司董事协会 (NACD), 2014年12月3日，http://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=12551.

[8] Ibid.

解答三个关键性问题

董事会如何在网络安全治理方面发挥更大作用，如何确保高效、快速的信息流？为此，董事会应积极主动地参与治理工作，了解最新动态，并确保对于网络安全保持着持续关注。在向董事会提供服务和指导的过程中，我们发现高管人员和董事会成员经常问到以下三个问题：

1 **新近出现的网络安全威胁和风险有哪些？它们如何对企业产生影响？**

第一个问题是从业务流程和企业目标角度考虑企业战略。解答这一问题，可使企业详细了解当前网络威胁的整体形势，即使面对繁杂的技术术语，也能在制定核心业务战略时确定网络安全战略。

2 **网络安全计划能否应对当前、未来的网络威胁所引发的挑战？**

第二个问题是从程序、（技术）能力和流程角度来解决战术问题，以及如何把这些事项传达至企业的各个层级。它关注企业是否采取了足够审慎的态度，以便依据风险等级缓释网络风险。

3 **哪些风险指标必须由高级管理层和董事会来审核，以便有效管理网络风险？**

第三个问题解决的是操作事项，明确风险指标，按优先级排序，从风险立场角度发挥出风险指标的真正价值，从而实现透明、持续的信息流。企业管理层必须付诸实践才能确认所做的事是否正确，也才能高枕无忧。

上面三个问题是相互关联的，兼顾了持续同步和整合两个因素，便于董事会机敏、灵活地应对不断变化的网络威胁。

毕马威全球网络成熟度框架

网络安全已不仅是技术问题，而是一个关乎企业全局的问题。为此，毕马威专门设计了全球网络成熟度框架，通过整合当前最具关联性的国际网络安全准则和治理准则，帮助企业解决网络安全的关键问题。

毕马威全球网络成熟度框架中可选择的IT或控制驱动因素极具价值，我们认为全球网络成熟度框架可以更广泛、深入、全面地解决董事会的参与度问题，以及指导董事会如何行使监督职责。

例如，美国国家标准技术研究所（NIST）制定的网络安全框架尽管有助于界定和评估当前环境下网络程序操作的控制成熟度，但毕马威全球网络成熟度框架可以在董事会与非IT领域的监督和治理之间架起一座桥梁，使二者更加协调。同时，这两个框架还可相互兼容。

我们定期为董事会提供多领域评估，特别建议从以下六方面来考查企业的全球业务：1. 领导和治理；2. 人员因素；3. 信息风险管理；4. 业务连续性和危机管理；5. 运营和技术；6. 法律合规。

将上述六方面相整合的全局模式可产生以下优势效应[9]：

- 减少企业受外部网络攻击的可能性，并缓解网络攻击产生的不良后果。
- 更好的进行网络安全决策，网络防御措施、网络攻击模式和事故响应方面的流程和条款得以完善。
- 使网络安全事项的沟通渠道更加清晰。员工了解自身职责以及在网络安全事件（或疑似事件）发生后应采取的措施。
- 提升企业信誉，在网络安全领域经过认真思考并做好准备的企业将激发利益各方的信心。
- 提升网络安全领域的知识和能力。
- 提升企业在网络安全领域的标杆地位。

此外，我们提供框架匹配服务，使全球网络成熟度框架与企业的其他框架实现兼容。

[9] *Cybersecurity*, a theme for the boardroom, p. 17, 毕马威企业咨询 N.V.（荷兰），2014年，由毕马威合伙人John Hermans编撰，
http://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Pages/Cybersecurity-a-theme-for-the-boardroom.aspx

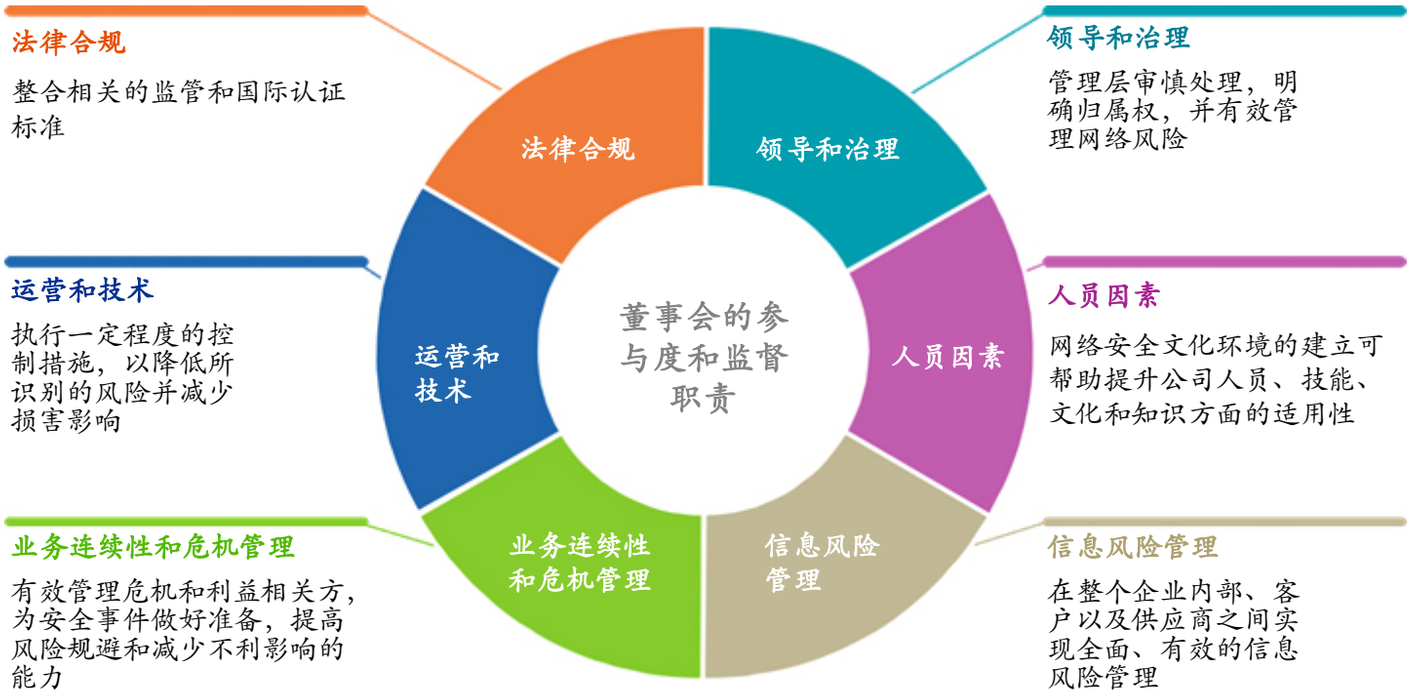
毕马威全球网络成熟度框架：六个领域

全面、深入地帮助董事会行使监督职责

六个领域的沟通和指导流程

在网络成熟度框架下，一份良好的沟通计划应体现出董事会与管理层之间持续沟通和指导的细节信息和复杂度。它有助于利益各方之间实现真实、可靠的信息流。这不仅要求对沟通频率进行重新评估，同时需要在应对风险时提高沟通的效率和质量。网络成熟度框架遵循的原则是，将安全状况视为与最薄弱的环节相等同，而最薄弱的环节往往是人员，不论薄弱的原因是由于知情人员、人为错误还是其他的人员因素。

最终目标是让技术、法律、战略或运营上的所有沟通共同为利益各方带来优势效应。企业提出的问题应当正确，具体内容也必须为每一位相关人士带来真正的价值。毕马威开发的创新型框架，可帮助企业打造适当的对话机制，并从总体上提升信息流的透明度和持续性，实现信息的高效流转。



I. 领导和治理

管理层审慎处理，明确归属权，并有效管理网络风险

董事会如何参与?

- 了解治理架构，与高级管理层持续沟通
- 审核能力评估结果
- 审批战略和资金申请
- 实施一般性的指导
- 要求定期进行方案更新

沟通

指导

- 明确方案的归属权和治理架构
- 识别敏感性数据资产和关键基础设施
- 清查第三方供应商关系
- 评估当前的能力状态
- 制定相关战略和方法
- 指导董事会成员和高级管理层

管理层应做什么?

II. 人员因素

网络安全文化环境的建立可帮助提升公司人员、技能、文化和知识方面适用性

董事会如何参与?

- 制定文化基调
- 审核人员事项的模式/趋势
- 了解培训和宣传方案

沟通

指导

- 制定文化和期望
- 实施一般性培训和宣传课程
- 实施人员安全措施
- 制定人才管理和职业发展架构
- 为关键人员制定学习路径

管理层应做什么?

III. 信息风险管理

在整个企业内部、客户以及供应商之间实现全面、有效的信息风险管理

董事会如何参与？

- 了解风险管理方法与风险之间的联系
- 核批风险容忍度
- 了解第三方供应商计划
- 复核并质询计划指标

沟通

指导

- 制定风险管理方法和政策
- 识别风险容忍度并进行相关沟通
- 将风险与敏感性数据资产相关联
- 执行风险评估和计量
- 实施第三方供应商认证
- 报告相关指标

管理层应做什么？

IV. 业务连续性和危机管理

有效管理危机和利益相关方，为安全事件做好准备，提高风险规避和减少不利影响的能力

董事会如何参与？

- 了解当前的应对能力
- 复核整个计划的成熟度
- 约见沟通人员
- 参加模拟演练

沟通

指导

- 评估当前的网络事件管理能力
- 分析风险和相关财务要求
- 制定完善的计划
- 分配资源并安排培训
- 融入企业的沟通过程
- 执行计划测试

管理层应做什么？

V. 运营和技术

执行一定程度的控制措施，以降低所识别的风险并减少损害影响

董事会如何参与？

- 了解当前控制框架的成熟度
- 审核控制框架样本的关联性
- 复核相关的事件趋势指标
- 约见信息总监或类似管理人员，了解网络和信息技术趋势的整合情况

沟通

指导

- 选择并实施控制框架
- 落实逻辑和物理安全控制措施
- 进行安全威胁和漏洞管理
- 进行安全监控
- 落实事故应变方案
- 根据广泛的IT服务管理环境整合各项活动

管理层应做什么？

VI. 法律合规

整合相关的监管和国际认证标准

董事会如何参与？

- 了解与企业相关的监管规定
- 明确审计委员会在网络安全方面的职责和要求
- 审核诉讼存量趋势
- 核批网络保险资金（如相关）

沟通

指导

- 列出所有相关的合规要求
- 将合规要求与控制框架相关联
- 正式制定审计委员会的作用和职责
- 开展诉讼存量和趋势分析
- 分析网络保险的必要性并提供建议

管理层应做什么？

将关键点与指标相对接

企业应运用关键绩效指标持续评估、度量框架的价值：哪些指标应纳入网络风险“仪表盘”？企业是否完成了既定的网络风险防控目标？关键绩效指标如何与同行企业的关键绩效指标相对接？

案例分析

推进董事会网络安全监督

2014年初，一家全球大型制造企业在知识产权管理方面出现安全漏洞，但直到美国联邦调查局发出警告才意识到这一问题，当时联邦调查局正在监控大量数据向境外知名黑客系统转移的情况。初步分析违规事件后，管理层需要与董事会进行解释和沟通，由于事情仍在不断发展，因此每天都有新情况需要沟通。

在事件发生前，董事会仅从信息总监IT年度更新中得知网络安全的大致情况。现在的董事会变得更加主动，开始深入了解企业面临的网络安全风险，以及未来如何管理这些风险。

公司聘请毕马威网络安全团队对董事会进行培训指导，并对公司员工、流程和技术控制进行网络成熟度评估，以降低网络威胁和风险，初步报告完成后被交至董事会。报告不仅按优先顺序列示了全面整治路线图，以解决短期内的安全缺口，同时提出长期战略，指导公司应对不断变化的网络安全威胁。

按照路线图进行资金分配后，董事会在持续关注当前运行状态的同时，也要求管理层每季度汇报安全方案进展情况。在毕马威的协助下，管理层制定了关键绩效指标“仪表板”；但是，由于受违规事件的影响以及董事会职责意识的提升，董事会并未止步在审核管理层书面材料的层次上，而是聘请毕马威网络安全团队按季度对进展情况执行独立的“健康检查”，并核查关键指标列示的部分信息。在工作过程中，毕马威网络安全团队持续协助审计委员会，出席所有会议，就新趋势提供培训指导，同时核证管理层的认定。最终，董事会的监督职责趋于明确，公司也建立了明确的流程，推动管理层与董事会进行交流和指导。

结语

- 董事会对网络安全的监督需要高管的积极参与。
- 网络安全治理计划需要将董事会职责变化因素考虑进去，同时兼顾沟通的频率和有效性。
- 通过解答三个常见问题完成信息流的透明、持续流转，以解决战略、技术和运营上的问题。
- 毕马威开发的全球网络成熟度框架从6个领域协助企业广泛、全面地推进董事会行使监督职责。
- 企业制定的框架应确保在企业内部实现高效、适当和持续的沟通与指导。
- 了解基准框架指标带来的价值提升，按照行业准则将指标与企业框架进行一一匹配，使企业保持积极主动，维护信息流的透明、高效、持续流转。

笔记

毕马威网络安全团队简介

毕马威网络安全团队旨在协助全球企业改造安全性、隐私性和连续性控制，使其成为业务支持的有效平台，同时保持主要职能的保密性、完整性和可用性。毕马威网络安全团队将根据客户的业务重点与合规需求提供解决方案。

联系我们

石浩然
网络安全合伙人
毕马威中国
电话：+852 2143 8799
邮箱：henry.shek@kpmg.com

梁景丰
网络安全总监
毕马威中国
电话：+852 2847 5052
邮箱：kk.leung@kpmg.com

崔巍
网络安全总监
毕马威中国
电话：+86 (10) 8508 5470
邮箱：calfen.cui@kpmg.com

张令琪
网络安全总监
毕马威中国
电话：+86 (21) 2212 3637
邮箱：richard.zhang@kpmg.com

kpmg.com/cn/cyber

本文是“Connecting the dots: A proactive approach to cybersecurity oversight in the boardroom”的修订版，作者是毕马威美国分所的Greg Bell和Tony Buffomante。