网络风险管理：重心转向治理

银行治理领导网络

Tapestry Networks

EY 安永

Building a better working world

网络风险管理：重心转向治理

“企业的对手换了一批又一批，但不变的是，总有些人对你虎视眈眈，其中包括黑客、有组织犯罪乃至某些长期以来一直筹谋此道的国家。这是一种动态的、不对称的风险。”——与会者

近年来，银行开始加大对网络风险的关注力度，大幅提高对网络安全的投资。尽管如此，近期的一项风险专业人士调查显示，网络风险和数据安全仍是2017年的首要操作风险关注点。[1] *“网络威胁与日俱增。随便读一份报告，你就能看到其影响。网络威胁不断变化，且越来越严重，”*一位董事表示。事实上，国家行为者篡改选举数据并组织攻击以银行为主的诸多公司等新闻头条屡见不鲜。[2] 客户、投资者和监管机构都希望确保董事会了解相关风险，并竭尽所能确保银行已经采取相关管控措施。

银行治理领导网络在几个月的时间内举办了多次会议，包括2017年2月23日和3月16日分别于纽约与伦敦举行的会议。与会者在会上分享了董事会和风险管理团队在网络安全监督方面遇到的实际挑战。本期《视点》[3] 总结了会上提出的观点与理念，以及董事、高管人员及监管者和银行业专业人士之间近30次事先会谈内容。参与讨论的人员名单见附录1。同期还发布了《视点》系列刊物《银行业转型：非金融风险监督在技术和业务模式转型中不可或缺》，重点阐述了有关其他非金融风险和转型议程管理的内容。从上述讨论中得出的重要主题与洞见概述见以下各章节：

- **网络漏洞为风险管理和监督带来独特挑战**
- **监管机构在明确网络风险预期方面更加规范**

网络漏洞为风险管理和监督带来独特挑战

由于网络风险不断变化且数字化银行业务导致的漏洞与日俱增，网络安全仍是董事会在风险监督方面面临的特别挑战。一位与会者指出，*“所有大型金融机构都已意识到自身在应对网络风险方面的弱势，并为此投入大量资源。我们与不同的国家和国际机构密切合作。我认为我们已经竭尽所能了。”*那么董事会如何才能知道他们所采取的措施是否充分呢？一位高管提醒称，*“在网络风险得到有效管控之前，你的耐心就会耗尽……我们尚未做到有条不紊。”*

“在网络风险得到有效管控之前，你的耐心就会耗尽。”

——与会高管

设定风险容忍度

金融机构的领导者们普遍认为无法百分之百杜绝网络漏洞。他们中的很多人正在尝试针对网络风险的各个方面设定风险偏好或容忍度。而此任务充满挑战。一位董事表示，*“我们的信息安全现状导致我们一直处于违反风险偏好的状态中。我们并不清楚自己能否处理不断变化的威胁。尽管已经采取了一些措施，但我们一直在违反自己的风险偏好，我们很清楚这一点。”*一些董事询问如何才能确保采取了适当的措施应对网络风险。一位董事承认，*“除了表明正在研究整改项目之外，你什么都做不了。”*一位与会者表示，设定网络风险容忍度时面临的一项特别挑战是*“网络风险并不对称。坏人只要成功一次即可，而你却必须始终保持无懈可击。”*此外，一位与会者指出，*“某些类型的威胁是无法减轻的。如果某个国家特别针对你采用了先前未知的策略，那么你不得不面对。”*这一挑战表明，对于董事会和高管团队而言，了解所面临的风险范围、应采取的特定缓释措施以及如何将风险和缓释措施与其风险偏好保持一致是多么重要。

> *“坏人只要成功一次即可，而你却必须始终保持无懈可击。”*
>
> ——与会者

了解所需的投资

*“如果你意识到无论如何都会发生网络攻击，你的风险容忍度就不可能为零，那么问题来了，你愿意为此花费多少钱？答案是投资巨大，”*一位与会者表示。另一位与会者分享了一些历史背景：*“许多大型银行在五年前就掌握了主要的网络安全能力。他们为此投入了大量资金。尽管如此，仍存在许多数据漏洞。这是为什么呢？因为这些能力并不成熟，而且是在孤立状态下实施的。我们发现，薄弱环节大多出现在相互联通方面。这为网络攻击者提供了新的机会。”*而这种持续的脆弱导致的结果就是，很多董事会都认为其首席信息安全官（CISO）*“总是告诉我们，网络环境极其糟糕，我们需要大量投资，”*一位与会者表示。一位高管指出，*“作为风险专业人士，我们必须为董事会提供更好的衡量进度的方法，否则他们将失去耐心，”*但他补充道，*“眼下我们确实需要大量投资。不断要钱的首席信息安全官也确实需要资金。”*许多大型银行开始逐渐加大对相关工具的投资力度，例如，自动化关联引擎，该工具可收集和消化不同来源提供的海量数据，以预测、识别和响应网络攻击。[4]

> *“……不断要钱的首席信息安全官确实需要资金。”*
>
> ——与会高管

尽管董事们因未能计量网络支出的有效性而受挫，但一位董事针对过于关注精确计量的现象予以提醒：*“我们需要牢记该项活动的总体目标，而不是过于关注‘我是否可以把投入的钱数与加强管控联系在一起？’”*

识别威胁、修复漏洞

跟上网络威胁的变化步伐仍是一项艰巨挑战。董事们无需成为网络安全领域的专家，但确实需要了解银行所面临的风险和适当的应对措施。专家们通过调查破坏原因来区分威胁是来自破坏分子还是来自黑客；犯罪分子的目标是钱，通常会通过勒索软件发起网络攻击；间谍的目标是知识产权；破坏分子的目标是造成实际破坏；而消极怠工者是指那些只是懒惰和不遵守安全协议的员工。一位与会者表示，*“每个攻击者的动机都会让你采取不同的防御策略。”*

一位与会者指出，让问题更加复杂的是：*“网络攻击的成功不是一蹴而就的，而是一个漫长的过程。”*因为最终难免出现漏洞，因此管理网络风险并不仅仅是做好防御，而是关乎*“如何防御、应对和恢复，涉及整个周期。”*包括审查系统备份的结构设计方式和备份数据存储位置等措施。一位与会者指出，*“大多数的网络设计旨在鼓励交叉销售和便于用户使用，因此很容易入侵。”*这意味着，银行必须设法*“拦截风险”*，例如，在网络攻击者入侵公司网络后，通过*“改变经济活动，使网络攻击者取得成功的代价更高。”*他们可能将虚假服务器作为诱饵，或考虑如何在服务器之间使用防火墙。一位与会者提醒称，*“网络攻击者很聪明，他们会关注流程。他们甚至可能会先攻击备份数据。”*与会者还关注数据的存储位置和存储方式。一位董事表示，*“由于我们鼓励创新，越来越多的人将数据存放在首席信息官都不知道的地方。”*随着越来越多的银行将数据迁移到云端，董事应考虑云服务是私有的还是公有的，以及云服务处于哪个管辖区。

> *“由于我们鼓励创新，越来越多的人将数据存放在首席信息官都不知道的地方。”*
>
> ——与会董事

系统威胁或许比个别银行漏洞更令人担忧。一位与会者指出：*“许多大型网络攻击之所以还未发生的原因在于，恐怖分子还没有真正转战网络。虽然某些国家已经转向网络攻击，但阻止他们比较容易。恐怖分子的目标是发动恐怖行动。破坏行动不难实施，但通过网络攻击发动恐怖行动却很难。但是这也只是时间问题。”*先进网络工具的市场需求不断增长，一些机构打出为最高竞标者提供精密黑客工具的广告。同一与会者指出：*“问题的关键并非缺少工具或能力不足，而是缺少动机和缜密性。”*一位与会者提醒称，犯罪分子*“越来越热衷于攻击网络基础设施本身。”*

完善治理和监督

各家银行采取的网络风险监督方法不尽相同。一些银行让技术和风险委员会分担董事会的主要责任。另一些银行则组建了专门关注网络安全的子级委员会。大多数银行指定了一名负责网络弹性的首席信息安全官。然而，针对网络安全官的汇报结构仍存在分歧。*“有人认为该职位应向首席风险官汇报工作。当时我就在想，这是什么逻辑？之所以会存在风险是因为信息技术问题。如果是我来确定汇报路径，我一定会确保网络问题应汇报给首席信息官（CIO），”*一位董事表示。

与会者强调了他们认为能够提高董事会治理有效性的方法，包括：

- **鼓励组织上下形成网络意识文化。**近期，《经济学人》中的一篇文章阐述了网络安全会构成文化挑战的原因：*“人们很容易相信，采用更多技术手段以及呼吁增强警觉性就可以解决计算机安全问题……这需要培养对计算机安全问题极其重视的偏执态度，因为对于非科技企业来说，这种态度并不是与生俱来的。”*[5] 近期的数据表明，近三分之二的网络漏洞归咎于员工的疏忽或恶意行为，因此这一点尤为重要。[6] 一位与会者提出这样一个问题，*“如何将弹性植入企业文化的DNA，从而让每位员工都了解自身行为的后果？最终，人们应该将网络视为一项基本技能。并不是要求每个人都要成为专家，而是要求每个人都需要具备情景感知能力。”*另一位与会者表示，*“安全问题始终需要权衡取舍……我们的目标是将大家的思维模式从关注不犯错，转变为充分调动所有员工，让每一个人都成为发现安全问题的传感器。你无需要求所有员工都避免点击钓鱼网站链接；你只需要有一名向你汇报问题的员工。”*另一位与会者则重点关注控制和扩大风险管理职责事宜：*“将这些风险转化为有效的控制策略是其中一项挑战。把责任分配给三道防线是驱动方向。而以前的情况并非如此。”*

“你无需要求所有员工都避免点击钓鱼网站链接；你只需要有一名向你汇报问题的员工。”

——与会者

- **增加董事会了解网络专业知识的途径。**大多数董事会正在试行新的治理架构，例如，组建专门委员会并引入网络安全顾问，或增加咨询委员会，考虑如何最有效地划分委员会和董事会之间的监督职责。其他董事会则纳入具有网络专业知识的董事。一位董事表示，*“我们引入一名没有任何金融机构从业经验的网络专家，因此，该专家需要反复了解业务运行方式。这样做的价值在于，该专家能够与首席信息安全官顺畅交流。他们背景相同，因此能够将沟通的内容有效传达给董事会。”*然而，董事们也提醒不要过度依赖董事会中的专家。一位董事表示，*“不可能找到了解一切技术发展问题的董事会成员，但重要的是找到可用的专家。”*

- **确保高管层面的问责机制和优先事项。**一位与会者建议，*“持续施压。我知道每家银行都有首席信息安全官。所有人都认为他们重点关注网络安全问题，但真正需要他们的时候，他们的表现往往令人失望，尤其是当网络安全与机构优先事项相互矛盾的时候。”*另一位与会者指出，*“高级管理层是最难管理的团队之一。在安全事宜上他们享受特殊待遇吗？如果享受，那么需要调查这些特殊待遇是否有必要……无需为首席执行官（CEO）提供超级用户访问权限。”*

- **制定健全的应对及恢复计划。**与会者一致认为，银行应该制定适当的应对计划并借助情景做好准备工作，藉此降低不可避免的网络事件的影响。一位与会者指出：*“通常，我们在董事会上听取违反网络安全制度可能导致的问题，然后了解‘发生了什么’。但可能直到六个月之后，你才真正了解发生的事件、方式以及原因。资源投入的实际目的是缩短这一过程。”*情景规划和“实战模拟”虽然在细节上不能映射真实事件，但却能够有所

帮助。董事会的优先事项包括了解自身在事件中的角色。例如，董事会应在多久之后提醒公众出现重大漏洞或数据丢失？一位监管者提出这样的问题，*“假设出现重大安全漏洞，可能会导致勒索攻击。你是否会支付赎金？你打算什么时候告知客户？”*另一位董事抱怨各类信息参杂在一起，*“监管机构让你告诉客户，而警方让你什么都不要说。”*一位监管人士解释说，*“提供给外界的反馈十分复杂，人们就此会做出假设。银行不同于其他企业，对于银行来说，最重要的是信任和安全。我们是在安全问题上犯错。如果我们对外透露了消息，但结果证明这些消息是错误的，那么我们将失去整个体系对我们持有的信心。我们考虑自身在应对安全问题方面的作用。我们确实认为大家需要通力协作。”*

“如果我们对外透露了消息，但结果证明这些消息是错误的，那么我们将失去整个体系对我持有的信心。”

——监管人士

监管机构在明确网络风险预期方面更加规范

一些分析指出，由于金融行业在防御措施方面加大了投入，因此整个行业的网络安全成熟度处于领先水平。[7] 但仍有许多政策制定机构担心金融行业做的还远远不够。前美国财政部副部长Sarah Bloom Raskin指出，尽管与其他行业相比，金融服务行业可能已十分出色，但仍存在许多不足，她认为*“许多现成的最佳实践”*并未得到普遍推广。[8] 目前，并不缺少相关框架和指引。近期发布的报告指出，各级别的监管机构以及行业团体 *“针对金融服务行业联合发布或拟定了43条互不重叠的网络安全框架、调查问卷、规则和要求。”*[9] 许多机构除遵循合规指引外，同时还实施了一些规定，美国国家标准技术研究所（National Institute of Standards and Technology, NIST）框架便是其中之一。[10] 一位监督人士表示，目前银行仍未达到NIST标准：*“我们已经根据 NIST框架进行了相关检验。没有一家机构符合我们的预期。银行业的现状也无法让人满意。他们还在苦苦应对一些基本问题。”*

美国新出台的网络法规将重心转向治理和控制

美国联邦存款保险公司、货币监理署和联邦储备系统以*“拟定法规预先通告”*（Advance Notice of Proposed Rulemaking, ANPR）的形式，联合发布了针对金融机构的加强网络风险管理标准。安永在一份简报中指出，该拟议法规要求银行确立经董事会批准的网络风险管理策略以及董事会的网络风险偏好。此外，金融机构应对所有经营性资产和资产重要性以及对外部依赖的实时掌控能力进行统计。[11] 一些与会董事认为，和监管机构之前的指引相比，*“拟定法规预先通告”*涉及范围更广，要求更加严格。但一位与会者认为，作为包含多个阶段的意见征求流程的第一步，该提议有意扩大涉及范围，以获取反馈，最终版规则的范围很可能会缩小。大多数与会董事表示，此拟定准则并不会创建新预期或大幅提升当前预期，造成预期远远超过董事会的工作现状，而是明确具体职责。该准则为监管机构带来了新的工作重点，正如一位与会者指出：*“之前的网络监管重点都在于预防。而此规定更加强调治理模型的建立。”*

“之前的网络监管重点都在于预防。而此规定更加强调治理模型的建立”

——与会者

一位与会者对此加以详细说明：*“‘拟定法规预先通告’包括了关于三道防线以及同董事会沟通的第二道防线的叙述。重点在于如何联合第一道和第二道防线。然后通过内部审计验证网络风险框架是否符合监管规定……‘拟定法规预先通告’必须由董事会来管理……‘拟定法规预先通告’中的许多规定都十分合理，但其涉及的范围值得商榷。例如，它强制要求你要对供应链有所了解。”*另一位与会者总结道，*“‘拟定法规预先通告’为整个机构的网络安全管理提供了明确指引。例如，如果你从事一项收购业务，那么你该如何看待网络风险带来的影响？该通告的目的是确保机构必须管理网络风险，而非接受它。‘拟定法规预先通告’旨在启发人们从端到端的视角去看待网络。”*

*“拟定法规预先通告”*是七国集团监管人士与政策制定者们的讨论成果的副产品。其他国家的监管机构有可能对此加以借鉴，制定类似要求。此类要求或许不像*“拟定法规预先通告”*那么规范，但会基于类似的一致性原则。

欧洲数据法规即将生效

欧盟新的《一般数据保护条例》（European General Data Protection Regulation）将于2018年5月生效。一位与会者对此评论到，*“这项条例旨在保护欧盟公民的个人数据，要求十分严格，处罚力度相当大。如果你在欧洲经营企业，一定要确保企业按要求制定了相应流程。否则你需要按违规类型缴纳罚金，最多可能要缴纳年营业额的4%。”*与会者们被提醒不可低估这些要求的重要性。*“法律要求大多数机构明确应对措施。但战略性挑战十分广泛。如果风险没能得到正确处理，机构可能会陷入麻烦……每家机构都会受此影响，”*一位与会者提醒道。

与会董事接受更高的监管期望，但希望避免重复监管

一些与会董事表示，监管机构只能视银行和董事会为问责对象。一位与会董事评论道：*“我认为监管机构并不了解技术方面的问题。他们身处严苛监管的原则之下，不断要求董事会加强监控，增强治理和承担责任，而没有关注到问题的具体细节。但我确实认为迫使金融机构就此进行内部讨论的决定十分正确。”*另一位与会董事说：*“我们都知道监管期望已大幅提升，甚至在新规则制定之前就要求我们有所作为。监管期望通常要求你持续保持最高技术水平，但是这个最高水平不断演变……监管机构给我们布置了一系列的新任务，工作量极大。”*

“……监管期望通常要求你持续保持最高技术水平，但是这个最高水平不断演变”

——与会董事

尽管对此普遍接受，但与会者建议监管机构将工作重心放在能够产生积极影响和提升标准的议程上。一位与会董事提醒道，*“我们当中大多数采用NIST工作标准。如果监管指引与该标准存在不一致，监管机构要为此给出明确理由。世界上大约有65家监管机构都在为此制定相关指引。真的过于复杂。”*

★ ★ ★

行业专家预测，网络风险正逐渐成为这个时代的*“主要问题”*——其意义和重要性堪比气候变化，为此，银行需承诺在未来数年投入大量资源。[12] 网络风险在过去常被视为技术问题，主要通过技术解决，并未被视为需要董事会应对的战略性威胁。但那个时代已经成为过去。随着技术逐渐嵌入银行业的各个方面，银行的网络风险也随之扩散，越来越需要董事会的密切关注。一位与会者对银行领导层所面临的网络安全和相关问题的重要性进行了概括：*“董事长和首席执行官能对投资者说‘我们并不打算重点防御这样或那样的风险’吗？或者，他们会因为网络风险日趋加大而放缓客户创新吗？或就数据收集表明立场吗？我们的董事会是否会针对网络风险的深入影响承担责任？还是像一位与会者所说，技术行业是否在推动我们的意识更新？这会影响我们的重要战略选择。”*

“我们的董事会是否会针对网络风险的深入影响承担责任？……这会影响我们的重要战略选择。”

——与会者

关于银行治理领导网络（BGLN）

银行治理领导网络致力于解决复杂的全球性银行所面临的关键议题。它的主要关注对象为非执行董事，同时也包括致力于实现卓越治理与监督的高管成员、监管机构及其他关键利益关联方，从而为构建强大、持久和值得信赖的银行机构提供支持。BGLN由Tapestry Networks在安永的支持下予以组织和领导。《视点》（ViewPoints）由Tapestry Networks创办，旨在捕捉BGLN讨论及相关研究的精髓。我们希望《视点》的接收者在各自的人脉圈中与他人分享相关内容。参与这一前沿对话的董事会成员、高管、顾问及利益关联方人数越多，《视点》为他们所创造的价值也就越大。

关于Tapestry Networks

Tapestry Networks是一家私营专业服务公司。其使命旨在提高社会跨部门、地域和地区实施治理与领导的能力。为此，Tapestry建立了由公共和私营部门及民间团体参与的多方利益关联方协作机制，这些行动的参与者均为各关键利益关联方组织的领导者，他们意识到当前的现状既无法满足需要，也无法实现可持续发展，因此正在寻找一个超越其自身利益而使所有人从中受益的目标。Tapestry已采用这种方法来解决公司治理、金融服务及医疗保健方面严峻而复杂的挑战。

关于安永

安永是全球领先的审计、税务、财务交易和咨询服务机构之一。我们的深刻洞察和优质服务有助全球各地资本市场和经济体建立信任和信心。我们致力培养杰出领导人才，通过团队协作落实我们对所有利益关联方的坚定承诺。因此，我们在为员工、客户及社会各界建设更美好的商业世界的过程中担当重要角色。安永为BGLN提供支持，作为其对实现金融服务业董事会效率及良好治理的持续承诺的一部分。

附录：银行治理领导网络峰会参与者

今年2月和3月，Tapestry Networks 协同安永共举办了两次BGLN峰会会议，探讨了银行在技术、业务模式和运营模式快速发展时期面临非金融风险监督挑战，并且同与会银行董事、高管、监管者、监督人员以及其他行业权威人士进行了大约50次会谈。会谈中提出的相关见解为本期《视点》提供素材，有些观点在本文中被多处引用。

以下为参与BGLN会议关于非金融风险性质不断变化的讨论的人员名单：

银行董事和高管

- Clare Beale，汇丰银行独立模型审查全球主管
- Bill Bennett，加拿大多伦多道明银行风险委员会主席
- Win Bischoff，摩根大通证券董事长
- Lord Norman Blackwell，劳埃德银行集团董事会主席、提名和治理委员会主席
- Jonathan Bloomer，摩根士丹利国际非执行董事
- Chantal Bray，汇丰银行养老金风险全球主管
- Juan Colombás，劳埃德银行集团执行董事和首席风险官
- David Conner，渣打银行风险委员会主席
- Sir Sandy Crombie，苏格兰皇家银行高级独立董事，集团绩效和薪酬委员会主席
- Sir Howard Davies，苏格兰皇家银行董事会主席，提名和治理委员会主席
- Nick Donofrio，纽约梅隆银行非执行董事
- Noreen Doyle，瑞士信贷董事会副主席、首席独立董事
- Dina Dublon，德意志银行风险委员会主席
- Betsy Duke，富国银行独立副主席
- Douglas Flint，汇丰银行董事会主席
- Tom Glocer，摩根士丹利运营和技术委员会主席
- Nick Godfrey，高盛常务董事、联席首席信息安全官
- Byron Grote，渣打银行非执行董事
- Mike Hawker，麦格理集团薪酬委员会主席
- Bob Herz，摩根士丹利审计委员会主席
- Olivia Kirtley，美国合众银行风险管理委员会主席
- Axel P. Lehmann，瑞银集团首席运营官
- John Lipsky，汇丰银行非执行董事
- Rachel Lomax，汇丰银行高级独立董事、行为和价值观委员会主席
- Douglas Lyons，野村国际首席信贷官
- Deborah McWhinney，劳埃德银行集团非执行董事
- Scott Moeller，摩根大通证券风险委员会主席
- Andy Ozment，高盛联席首席信息安全官
- Bill Parker，美国合众银行副主席、首席风险官
- Kevin Parry，全英房屋抵押贷款协会审计委员会主席
- Nathalie Rachou，法国兴业银行风险委员会主席
- Susan Segal，加拿大丰业银行公司治理委员会主席
- Alexandra Schaapveld，法国兴业银行审计和内部控制委员会主席
- David Sidwell，瑞银集团高级独立董事、风险委员会主席
- Tim Tookey，全英房屋抵押贷款协会风险委员会主席
- Jasmine Whitbread，渣打银行品牌、价值观和行为委员会主席

监管及监督人士

- Jonathan Davidson，英国金融市场行为监管局零售业务和授权部门监督主管
- Harald Heide，欧洲中央银行 DG- MS1/6a 部门主管
- Lyndon Nelson，英国央行审慎监管局副首席执行官兼执行董事、运营监管和风险监督专家
- Stephen Page，BSI 集团和英国国家犯罪调查局非执行总监
- Bruce Richards，纽约联邦储备银行高级副总裁，复杂金融机构监督事务负责人
- Molly Scherf，金融管理局大型银行监督事务副总审计长
- Todd Vermilyea，美国联邦储备体系监督和监管部高级副总监

安永

- Omar Ali，英国金融服务主管
- Peter Davis，美洲区金融服务咨询主管
- Marie-Laure Delarue，欧洲、中东、印度及非洲区银行业和资本市场主管
- John Doherty，治理风险与合规
- Steve Holt，金融服务咨询
- Ertem Osmanoglu，美洲区网络安全副主管
- Isabelle Santenac，欧洲、中东、印度及非洲区金融审计主管
- Bill Schlich，全球银行业和资本市场主管

Tapestry Networks

- Dennis Andrade，合伙人
- Jonathan Day，副董事长
- Colin Erhardt，副总监

尾注

[1] “2017年十大操作风险”，Risk.net，2017年1月23日。

[2] Emma Dunkley、Caroline Binham与 Sam Jones，90《金融时报》，2017年1月22日。

[3] 银行治理领导网络《视点》采用了《查塔姆宫规则》（Chatham House Rule）的修订版本。按照该规则，相关评论不归属任何个人、公司或机构。银行治理领导网络与会者的评论以斜体加以陈述。

[4] Steven Norton，“富国银行首席信息安全官表示网络投资为加强风险管理指明方向”， CIO Journal（博客），《华尔街日报》，2017年3月13日。

[5] “如何应对计算机安全威胁”，《经济学人》，2017年4月8日。

[6] “有效的网络安全策略依赖于人，而不仅仅是技术”，《保险杂志》，2017年3月1日。

[7] Jonathan Cedarbaum 与 Sean Reilly，“网络安全协作：提升防御的途径 ” 《银行业务视角》第3版，（2015）第一版， 第66页。

[8] Martin Arnold，“金融部门督促加大网络防御力度”，《金融时报》，2016年12月8日。

[9] Lalita Clozel，“大型银行致监管机构：不要践踏我们提升网络安全的努力”，《美国银行家报》，2017年3月1日。

[10] 美国国家标准技术研究所，“NIST发布网络安全框架更新”，新闻稿， 2017年1月10日。

[11] 安永，“加强金融机构的网络风险管理标准”，金融服务监管通讯，2016年10月。

[12] Eli Sugarman，“就2020年网络安全未来议题对Steven Weber提出的四个问题”，Hewlett Foundation，2016年5月23日。

联系我们

大中华区领导团队

陈凯

大中华区金融服务部

区域主管

+86 10 5815 4057

jack.chan@cn.ey.com

蔡鉴昌

亚太区金融服务部

审计服务主管

+86 10 5815 3222

geoffrey.choi@cn.ey.com

林安睿

大中华区金融服务部

审计服务主管

+86 21 2228 2929

aj.lim@cn.ey.com

梁成杰

大中华区金融服务部

银行及资本市场主管

+86 10 5815 3305

kelvin.leung@cn.ey.com

忻怡

大中华区金融服务部

咨询服务主管

+86 10 5815 3393

effie.xin@cn.ey.com

其他联系人

北京

许旭明

金融服务部

+86 10 5815 2621

steven.xu@cn.ey.com

上海

严盛炜

金融服务部

+86 21 2228 2332

ron.yan@cn.ey.com

深圳

张秉贤

金融服务部

+86 755 2502 8287

benny-by.cheung@cn.ey.com

广州

赵雅

金融服务部

+86 20 2881 2773

teresa.zhao@cn.ey.com

香港

涂珮施

金融服务部

+852 2846 9033

teresa.tso@hk.ey.com