Deloitte.

MFDF

共同基金董事论坛

网络安全和持续的环境威胁

共同基金董事的职责

2022年4月

因我不同
成就不凡
始于1845

目录

引言

共同基金董事必须采取行动应对网络犯罪数量和复杂程度不断上升的局面。此外，不断变化的监管环境加剧了网络安全监督方面的挑战。在这种情况下，基金公司必须尽力保护业务免受网络攻击带来的财务、品牌和监管影响。

网络威胁可能会在以下方面对基金公司、投资顾问及其股东产生影响：

- 财务：一起网络事件对组织造成的**平均损失超过100万美元**，[1]其中包括收入损失、知识产权损失、罚款等。
- 品牌：**65%**受数据泄露影响的客户会**对违规组织丧失信任**，而**33%**的客户会**与违规组织中断合作**。[2]
- 监管：监管机构正在加大执法力度，重点关注个人信息管理不当的问题。例如，对违反《通用数据保护条例》[3]的行为，罚款可能高达年收入的4%。

因此，实施有效的网络安全监督和治理计划对于管理网络风险和环境威胁至关重要。

共同基金面临的威胁日益增加

随着共同基金愈发依赖技术来开展运营，其所面临的网络威胁急剧增加。例如，使用数字应用程序的销售渠道可能会遭受更多的分布式拒绝服务攻击和客户数据窃取事件。勒索软件和数据窃取风险（包括客户数据和知识产权）在各类机构中普遍存在。这些威胁涉及以下方面：

- 前台运营（包括投资策略、特定交易算法、智能投顾和投资组合管理）；
- 中台运营（包括合规报告、支付与结算和风险模型）；
- 后台运营（包括基金会计、报告、人力资源、财务、营销）。

欺诈是另一种重大网络风险，可能由外部人员或恶意内部人员引发。例如，结算和财务系统以及财务部门使用的数据传输协议（包括SWIFT和FIX系统）可能遭到不当或不受监控的访问。

在未制定相关控制措施的情况下，增加机器人流程自动化（RPA）、人工智能（AI）和机器学习（ML）技术的使用可能会进一步暴露公司的网络漏洞。此外，将业务外包给第三方、与数字化转型工作相关的云服务提供商以及新冠疫情催生的远程工作模式也将扩大恶意行为者的攻击面。

资产管理行业为何成为攻击目标？

共同基金的结构提高了网络安全监督的复杂性。基金的主要职能和运营通常由第三方服务提供商负责，包括基金投资顾问和二级顾问、托管人、代销商、行政服务机构、过户代理人、会计师和帐户管理人。这些服务提供商都可能持有对网络犯罪分子具有吸引力的关键数据并且面临网络攻击的风险，从而在财务、品牌、声誉和监管等方面对投资顾问、基金公司及其股东造成巨大损失。

基金公司和投资顾问应当持续评估其网络风险敞口并且建立识别、检测、应对网络事件以及恢复业务流程和基础设施的能力（即制定正式的网络安全计划并严格实施以应对不断增加的网络风险）。

董事会的网络安全监督职责

基金董事不负责制定或监督网络安全计划，而是负责监督管理层和投资顾问开展的相关工作。尽管如此，董事会仍应保持警惕并就网络安全计划提出关键问题。

基金董事 (董事或董事会) 可能发现，从风险监督的角度审视网络安全将会有所助益。董事需要了解和监督基金管理人员和投资顾问如何管理风险，包括网络安全计划、全面风险管理和对基金服务提供商的监督。全面风险监督框架的原则可以为董事会履行网络安全监督职责提供指导。

基金董事必须依据州法规定履行职责，包括风险监督职责，以及其作为基金受托人的职责。作为受托人，董事对基金公司负有两项基本义务，即“勤勉义务”和“忠实义务”：

- 勤勉义务要求董事应根据其已掌握的专业知识及在担任董事期间获取的专业知识，谨慎行事。根据州法，董事通常可以合理求助专家，包括管理层、基金投资顾问、律师、会计师等。
- 忠实义务通常是指董事应当保护基金的最大利益，并且不得将个人或第三方利益置于基金利益之上。忠实义务还包括诚信义务。

法院通常根据“商业判断规则”评估针对董事的指控。在下列情况下，董事可以免于为其出于诚信作出的商业决策承担责任：1. 董事与商业决策主体不存在利益关系 (即不存在个人利益冲突)；2. 董事依据充分信息作出商业决策；3. 董事合理认为商业决策符合公司的最佳利益。

美国特拉华州大法官法院 (Delaware Court of Chancery) 的Caremark案件判决被广泛引用为理解商业判断规则的基准。[4] 该判决强调，董事可以建立并定期监测能够响应一般或特定监督议题的报告或信息流动机制，以此证明他们符合商业判断规则的标准。根据此框架，要求董事承担责任的案件通常声称董事会没有收到足够的信息来监督风险或者有意忽视向其报告的“危险信号”。

此框架在2018年被应用于某酒店公司因出现重大网络漏洞而面临的诉讼中。法院指出，虽然“公司因不遵守网络安全保障措施而遭受的损害促使董事确保公司建立适当的监督系统”，但是这些风险“**并未降低原告在向Caremark提出索赔时必须达到的高门槛**”[5] (重点补充)。在认定董事会的行为符合商业判断规则时，法院指出董事会进行了定期报告 (包括在年度风险清单中讨论网络安全风险) 并且了解外部顾问和内部人员都在致力管理网络安全风险，同时审查了董事会收到的与网络事件内部控制措施和应对计划相关的信息。

监管指引

监管机构正在加强审查基金公司为保护其组织和客户免受网络攻击而采取的措施。过去十年，美国证券交易委员会 (SEC) 和各州金融监管机构高度关注网络安全问题，美国政府还于近期发布行政命令和国家安全指令以应对日益严重的网络攻击。(本文重点关注SEC (共同基金的主要监管机构) 的相关要求，但是某些公司可能需要考虑相关的非美国监管指引) 。

SEC及其工作人员针对基金和顾问的网络安全监督工作提出相关要求所依据的监管指引包括：

- 投资管理部指导意见 (2015年更新) ，可以为董事会评估基金网络安全提供重要背景信息；[6]
- 多个监管检查部门针对网络安全问题出具风险预警和审查意见；[7]
- 企业财务部针对信息披露和内幕交易的指导意见；[8] 以及
- 针对基金公司和顾问的网络安全风险管理规则 (尚未通过) ，我们总结如下。[9]

SEC拟议网络安全风险管理规则 (第38a-2条规则)

2022年2月，SEC针对投资顾问 (《投资顾问法》拟议的第206(4)-9条规则) 和基金公司 (《投资公司法》拟议的第38a-2条规则) 提出了详细的网络安全风险管理规则。[10] 第38a-2条规则的核心是，基金公司必须针对网络安全问题制定书面风险管理计划。

当然，大多数基金公司已经制定了网络安全政策和程序。这些政策和程序可以反映SEC工作人员的现行指导意见、州法要求 (许多州已经要求制定 “书面信息安全计划”，有时称为WISP) 以及SEC S-P条例或S-ID条例下的信息保护和隐私规则。基金公司还考虑将网络安全防范纳入其根据第38a-1条规则 (合规计划规则) 制定的整体合规计划。无论SEC是否通过网络安全风险管理规则，基金公司都需要维护这些政策和程序。

拟议规则可能提出以下网络安全防范要求：

1. 采用与基金公司网络安全风险状况相适应的政策和程序，并任命一名或多名网络安全风险管理员来执行这些政策和程序。
2. 开展风险评估，包括评估与某些服务提供商相关的风险、监督此类服务提供商以及与此类服务提供商签订适当的书面合同。
3. 采取控制措施，最大限度降低与用户相关的风险并防止未经授权访问基金管理信息系统及其中的基金信息。
4. 监控基金管理信息系统并保护基金信息免遭未经授权的访问或使用，包括检测、减轻和补救网络安全威胁和漏洞。
5. 制定网络安全事件应对和恢复计划以确保：(1) 基金持续运作；(2) 基金管理信息系统及其中的基金信息得到保护；(3) 外部和内部沟通顺利开展；(4) 基金投资顾问根据SEC拟议保密报告机制报告重大基金网络安全事件；以及 (5) 事件得到书面记录。
6. 至少每年对该计划进行重新评估。

基金公司董事会需要初步审批该计划，并且收到 (至少) 一份年度书面报告。拟议规则规定的董事会职责和网络安全防范的总体框架与本文所述的监督结构和方法相一致。

治理架构和董事会职责

众所周知，高层参与对于有效实施网络安全计划至关重要。高级管理层应对制定网络安全战略给予充分重视。此外，董事会应对监督战略实施工作给予充分重视。在监管检查部门出具的报告中也对此进行了强调。[11]

如果获得通过，第38a-2条规则将对董事会监督提出具体要求。完成针对基金公司网络安全政策和程序的初步审批之后，基金公司董事还需审查网络事件报告以及政策和程序的重大变化。SEC在相关文件中一直强调："董事会监督不应是被动行为"。[12]

定期开展风险评估

鉴于网络安全威胁的性质不断变化，SEC工作人员意识到应对网络安全威胁开展动态评估。SEC工作人员建议投资顾问和基金公司了解与其业务相关的网络安全威胁和漏洞。[13]根据第38a-2条规则，基金公司将基于已确定的信息系统清单开展风险评估并根据风险评估结果对网络安全威胁进行分类和排序，同时了解不同服务提供商在维护和保护基金信息方面的作用。该规则将要求基金公司以书面形式记录风险评估结果。

评估潜在威胁可能需要了解：[14]

- 基金公司（直接或通过服务提供商）拥有的信息类型；
- 用于收集信息的技术系统；
- 信息和技术面临的内外部威胁；
- 如果系统遭到破坏，基金公司和服务提供商面临的风险；
- 为减轻网络安全风险而制定的控制措施和流程。

如上所述，基金公司董事将采用常规方法进行威胁评估并从业务角度考量各项威胁。例如，如果某个信息或技术系统可能遭到破坏，基金公司董事或将考虑公司的哪些业务职能将受到影响，影响程度如何，持续多长时间；威胁来源是什么；应当采取哪些首要缓解措施；以及公司将如何处理实际事件。[15]

制定网络安全策略

投资管理部工作人员建议基金公司根据评估过程中收集的信息制定网络安全威胁预防、检测和应对计划。[16]根据建议，该项计划可能包括：

- 数据访问保护；[17]
- 数据丢失预防；[18]
- 数据备份和检索；[19]
- 事件应对计划；[20]
- 网络安全策略定期测试。[21]

第38a-2条规则提出了类似要求，并且规定除上述风险评估外，基金公司的网络安全风险管理计划还应包括：

- 用户安全和访问标准，包括启用多因素认证（MFA）、设置密码程序、根据"必要知道"原则限制员工访问以及确保远程访问技术的安全；
- 信息系统定期评估，以此支持防止未经授权访问或使用数据的措施；
- 网络安全威胁和漏洞管理；
- 网络安全事件应对计划，旨在提高重大网络事件期间的运营韧性并就政府和客户报告提出具体要求。

有效实施战略

投资管理部工作人员建议网络安全策略实施工作应当包括：[22]

- 执行书面政策和程序；
- 对管理人员和员工进行有关威胁以及相关预防、检测和应对措施的培训；
- 开展投资者教育以降低其账户风险敞口。

除上述建议外，相关执法行动也可以就SEC对网络安全的看法提供有用信息。SEC执法部成立了网络部门，负责监控受监管实体的网络安全控制措施。在最近三次执法行动中，SEC对在基于云计算的电子邮件系统方面采取松懈网络控制和出现网络安全问题的八家SEC注册公司进行了处罚。[23]

投资顾问如何制定可持续的网络安全计划？

投资顾问和其他主要服务提供商可以根据各种框架制定网络安全计划。虽然深入了解此等计划不属于董事的职责范围，但是可以帮助董事会履行监督职责并确定关键问题。（本文经常提到“投资顾问”和“投资顾问的网络安全计划”，这体现了投资顾问在大多数基金公司中的核心作用，但是并不意味着基金公司不会制定自有网络安全计划，也不意味着贬低基金管理人员或除投资顾问以外的提供商在基金公司中的作用）。

国际注册专业会计师协会（AICPA, The Association of International Certified Professional Accountants）提出的框架可以帮助基金公司预防、检测和缓解网络安全事件，也可以为董事会履行监督职责和了解相关信息提供指导。该框架包括以下五个步骤：

- 确定需要保护的对象；
- 评估并划分职责；
- 建立风险管理流程；
- 采取应对措施；以及
- 不断总结经验。

下文旨在为董事会履行监督职责和了解相关信息提供潜在方法，而非支持任何特定框架。除AICPA提出的框架外，投资顾问和其他服务提供商还可以根据其他框架制定网络安全计划。此外，下列问题可能并不适合所有基金公司董事会；网络安全监督因基金的规模和复杂程度等因素而存在较大差异。

确定需要保护的对象

实施网络安全计划应从管理层或投资顾问确定关键资产 (例如信息、数据、个人信息、IT系统) 并评估潜在攻击者 (包括攻击方式、原因以及发生的相对可能性) 入手。

在评估投资顾问是否适当考虑了基金面临的网络安全风险时，董事可能需要考虑以下问题：

- 基金面临的最大网络安全威胁是什么?
- 哪些是我们必须保护的重要资产 (包括数据和其他资产) ?
- 清单是否涵盖基金运营所需的重要业务信息、个人信息和所有系统?
- 投资顾问是否了解网络攻击的潜在途径?

然而，鉴于基金行业的性质，投资顾问并非唯一需要董事会关注的实体。除基金投资顾问外，还有许多第三方也在为基金提供关键服务。这些服务提供商有权访问关键信息，很可能成为网络安全事件目标。为确定需要保护的第三方服务提供商的相关资产，投资顾问应当全面了解基金聘请的所有服务提供商，包括他们可以访问的信息以及与投资顾问自有系统和数据交互的方式。此外，了解第三方服务提供商是否将可能带来第四方及以上风险的业务外包或离岸外包也至关重要。董事可能需要考虑基金 (一般通过投资顾问采取行动) 是否拥有：

- 第三方服务提供商的完整清单；
- 第三方所收集、使用和/或维护的关键数据的完整清单；
- 监控第三方如何访问基金公司或投资顾问自有系统和数据的流程；
- 对将活动外包或离岸外包给其他方的理解；
- 针对基金第三方服务提供商带来的网络安全风险进行排序的流程。

评估并划分职责

配置适当人员并明确划分角色和职责对于有效实施网络安全计划至关重要。网络安全计划的有效性取决于该计划的负责人。投资顾问可以指派内部人员处理网络安全工作或将网络安全工作外包给适当的第三方。此外，投资顾问需要根据基金的规模、结构和复杂程度划分网络安全相关职责。

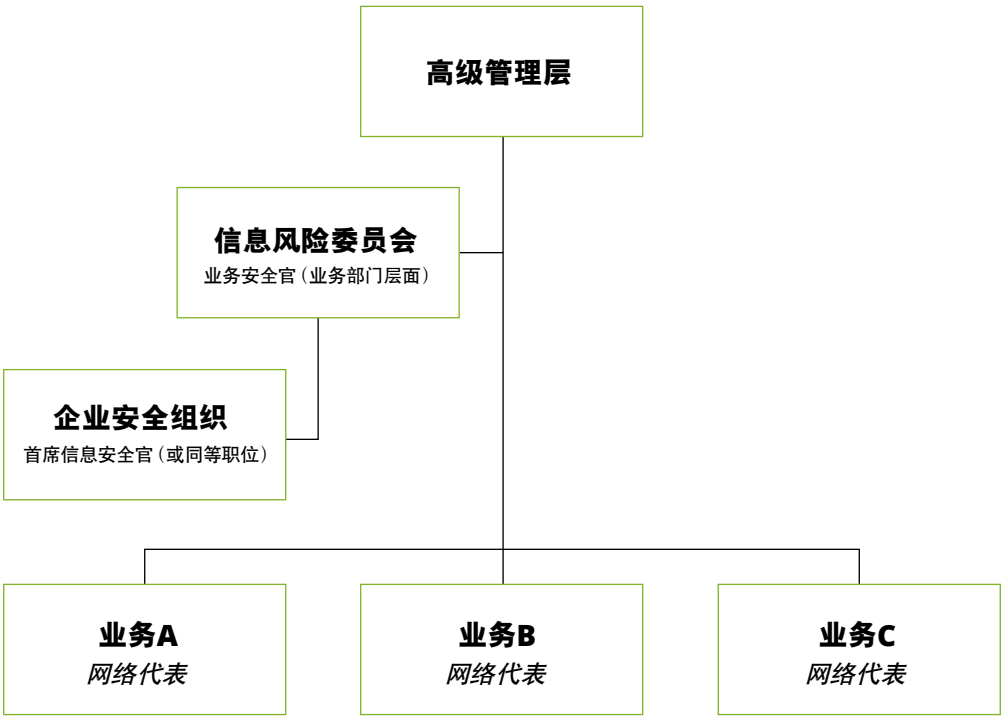
投资顾问需要确定如何针对网络安全计划进行人员配置——吸引内部人才制定计划或者聘请第三方处理网络安全工作。识别和聘请网络安全人员可能极具挑战。由于考虑因素太多，安全漏洞太多，而管理各项威胁的IT专业人员太少，许多组织被迫外包网络安全工作。根据德勤《2019网络安全前瞻调研报告》，85%的受访者表示在一定程度上依赖供应商和托管服务提供商来处理网络安全工作，其中三分之二的受访者外包了21%至50%的网络安全工作。[24]

就网络安全计划的人员配置而言，董事可能需要考虑以下问题：

- 投资顾问是否指派了内部人员处理网络安全工作？ 如果是
  - 投资顾问应如何评估这些人员是否接受了适当培训？
  - 投资顾问是否面临网络安全人员保留问题？
  - 投资顾问是否拥有实施网络安全计划所需的所有网络资源？
- 如果投资顾问聘请第三方服务提供商处理网络安全工作，董事可能需要考虑以下问题：
  - 投资顾问对所提供的服务水平是否满意？
  - 投资顾问开展了何种类型的初步尽职调查？
  - 投资顾问如何开展持续尽职调查？

配置适当人员（无论是内部人员还是服务提供商）之后，公司必须确定如何构建网络安全监督框架。与风险管理的其他领域一样，高层基调对于网络安全监督同样至关重要。无论对第三方的依赖程度如何，公司高级管理层都应在此过程中发挥关键作用。

某些组织已经意识到配置网络安全专业人员的优势。投资顾问机构的整合网络联系可以帮助公司针对优先事项达成一致，并且创建统一议程甚至避免对本可以预防的事件进行补救，这对投资顾问而言是一个新思路。如今，许多金融服务机构都在业务部门内部设置业务安全官。规模较大的投资顾问机构和其他服务提供商可以考虑采用类似结构（详见下图）。这与强调第一道防线管理企业风险相一致。



在评估投资顾问（或其他主要服务提供商）的网络安全工作时，董事可能需要考虑以下问题：

- 投资顾问机构的网络安全专业人员向谁汇报工作？
- 每个主要业务部门是否都配置了网络安全专业人员？如果不是，网络安全专业人员如何监控各个业务部门？
- 开发新产品或新服务时，业务团队如何与网络安全专业人员开展合作？
- 发生网络事件（或疑似事件）或规划新项目时，业务领导人是否知道应当与谁联系？

建立风险管理流程

确定公司的网络安全风险承受能力（有时也被称为“风险偏好”）对于制定有效的网络安全计划至关重要。该流程包括确定数字渠道中断时间的可接受水平；评估客户体验质量与安全性之间的平衡情况；以及评估客户使用的便利性等。完成全面评估之后，应将相关风险纳入公司的企业风险管理框架。为更好地理解网络安全风险承受能力及其对更广泛风险管理的影响，董事可能需要考虑以下问题：

- 投资顾问认为其网络安全风险承受能力如何？
- 关键网络安全风险是否根据风险承受能力来衡量？
- 网络安全风险工作如何为投资顾问提供更广泛的企业风险考虑因素？

投资顾问应根据其风险承受能力，制定相关政策和程序来管理组织的网络安全风险。由于基金的规模和复杂程度以及每个投资顾问的情况各不相同，因此各基金的网络安全风险管理政策和程序存在较大差异。在监督投资顾问的网络风险管理流程时，董事可能需要考虑以下问题：

- 投资顾问如何管理风险并确保将风险降低到可接受的水平？
- 管理层如何投入和分配资源以监控和防范网络风险并加快响应和恢复进程？
- 如何评估安全管理支出的回报和网络风险管理计划的有效性？

如上所述，投资顾问通常依靠其他第三方服务提供商来执行运营基金所需的日常职能。这些服务提供商可能会给基金公司和投资顾问带来相当大的网络安全风险；因此，管理这些风险对于制定有效的网络安全计划至关重要。有鉴于此，董事应当了解组织如何管理第三方带来的风险，并且可能需要考虑以下问题：

- 投资顾问是否建立了完整的自动化流程来提高第三方生命周期管理（包括接洽、尽职调查、合同签订以及对现有或新增第三方的持续监控）的效率和集成程度？
- 第三方监督职责是否已被纳入组织内部？是否已明确划分持续监控方面的角色和职责？
- 投资顾问是否提高了风险管理能力以及第四方和第五方控制措施的透明度？
- 投资顾问是否对第三方进行了主动的、智能驱动的网络威胁监控，包括具有针对性的数据保护审查，并提高了对第三方环境中托管组织数据的可见性？

采取应对措施

有效实施网络安全计划需要公司制定和执行相关政策和程序，以监督风险管理流程并应对不可避免的网络安全事件。网络安全计划不能防止所有网络安全入侵，但是应当可以检测入侵并在可行范围内减轻损害。

由于网络安全事件不可避免，因此投资顾问必须制定适当的危机应对计划。例如，该计划需要考虑投资顾问将如何应对危机，包括谁将采取何种应对措施，如何确保基金公司能够获得关键服务，以及在发生数据丢失时如何恢复关键数据。在评估网络安全事件防范情况时，董事可能需要考虑以下问题：

- 是否已为网络安全计划分配充足的人员和资金？
- 如何处理和报告事件？
- 如何测试网络安全计划？测试是否定期进行？
- 应对网络安全事件可以依据哪些协议？这些协议在整个组织中是否得到了明确和充分理解？
- 公司是否进行了模拟演习以提高对网络安全入侵的准备程度？
- 对于第三方服务提供商，公司是否深入研究了合同条款以确定各自对网络安全事件的责任？如果合同没有相关规定，是否商定了其他机制以在发生网络安全攻击时各司其职？
- 业务连续性和灾难恢复计划如何考虑网络安全问题？

网络安全计划的一个关键组成部分是完善的沟通机制。当董事会和投资顾问评估通信协议时，相关考虑因素包括报告计划，向董事会报告的关键人员，董事会履行网络安全监督职责的方式以及报告内容。董事会需要考虑的沟通相关事项包括：

- 采用何种报告计划？董事会和投资顾问确定的报告计划应当足以提供适当的监督保障。根据基金及其投资顾问的规模和复杂程度，董事会可以决定是在每次会议上进行报告还是采取其他适当的时间安排。除定期报告外，董事会和投资顾问还应确定何时向董事会报告关键网络安全问题。董事会和投资顾问可以根据事件的实际情况商定阈值和时间限制。
- 由谁向董事会报告？董事会和管理层还应当讨论由谁向董事会进行报告——首席信息安全官还是网络团队的其他成员。首席合规官可以帮助董事会根据待讨论的特定网络安全问题确定适当的报告人员。
- 董事会如何履行网络安全监督职责？董事会可能希望指定一个委员会承担主要监督职责，或决定由全体董事会成员共同承担该职责。如果董事会选择设立一个委员会来监督网络安全，该委员会应当考虑如何与全体董事会成员充分共享关键信息以促进有效监督。此外，董事会可以考虑指定专人负责在两次会议期间接收重大网络事件通知。
- 董事会将收到什么类型的报告？除确定网络安全监督职责履行方式外，确定适当的报告内容也至关重要。鉴于网络安全问题的技术性质，董事会必须与管理层合作，确保报告对董事会而言易于理解并且可为开展有效监督提供重要信息。

不断总结经验

随着基金不断变化和发展，其可能增加或变更第三方服务提供商以获得更优服务。此外，基金风险的性质可能会因基金管理使用技术的方式而发生重大变化。最后，网络安全威胁的性质并非一成不变——不良行为者正在不断改变网络入侵方式。因此，网络安全计划必须定期重新评估和更新以反映实际情况。评估投资顾问在此方面的行动时，董事会可能需要考虑以下问题：

- 投资顾问审查其网络安全政策和程序的频率如何？
- 投资顾问和董事会是否接受了关于新兴网络安全威胁的定期培训？例如，投资顾问可能会接受关于网络事件“根本原因”分析或行业网络事件“成因”分析的培训。
- 网络安全事件相关信息是否在整个组织中共享以使组织能够从过去的事件中吸取教训？
- 投资顾问是否参与了信息共享以便及时了解新兴威胁？

网络安全保险

鉴于网络安全事件可能造成重大损失，董事会或希望与管理层、法律顾问和保险经纪人讨论是否可以通过保险[25]弥补网络安全事件带来的损失和费用以及此类保险是否适合基金公司。

与网络安全的其他方面一样，随着保险公司获得更多专业知识以及网络安全问题不断演变，网络安全保险也在不断发展。就此领域而言，董事可能需要考虑以下问题：

- 谁持有保单？保单由投资顾问或其他服务提供商持有（而不是由基金公司直接持有）的情况可能更加常见。
- 谁是保单下的受保人？
- 保险范围包括哪些方面？是否有重要的免责条款需要考虑？
- 根据基金公司或投资顾问持有的基础保单，网络安全事件是否会按特定方式（明示或暗示）进行处理？
- 不同类型的保单（针对组织内的不同职能规定不同的保险范围并可能由不同的保险公司提供）将如何相互作用？

网络安全新兴领域

数字化转型推动网络演进

受市场需求和新冠疫情影响，大多数投资顾问和共同基金管理公司正在开展广泛而深刻的业务和数字化转型。董事会应了解转型工作的潜在网络影响以及投资顾问和主要服务提供商管理相关风险的方式。下文将重点介绍一些关键转型工作的网络影响。

自动化的便利性是否会带来更大风险？

基金开展业务转型的重点在于广泛应用RPA和人工智能（AI）/机器学习（ML）。RPA和AI/ML可以推动自动化，增强人工决策并快速创造业务价值。资产管理公司和共同基金管理公司正在加强RPA和AI/ML技术部署，以期通过自动化和分析工具提高流程效率。投资顾问也在利用RPA和AI/ML识别海量数据集中的常见特征或意外事件，整合细微数据洞察，并且实现快速和大规模数据解读。这些技术还有助于解决人力资源领域培训和运营成本不断上升以及熟练人才缺乏的问题。

然而，此类RPA和AI/ML技术的广泛应用增加了犯罪分子可以用于攻击组织的攻击媒介，并且带来了更大的安全挑战：

- RPA技术带来了新的攻击面，可能造成未经授权的访问。RPA软件通常需要特许访问权限（或高于标准用户的访问权限）才能执行任务。开发人员通常会将访问权限“硬编码”到脚本程序中，该过程可能包括从不安全的位置检索凭证的步骤。恶意内部人员或网络攻击者可能会窃取硬编码的可共享凭证，从而在网络中自由移动并访问加密数据系统。
- AI/ML增强功能将带来类似的网络风险。此外，训练机器所需的数据量也会提高网络风险。训练预测模型需要依靠大量数据；了解模型运行情况需要依靠测试数据；模型投入使用之后需要使用实时事务数据。
- IT组织可能会忽略训练和测试数据的数据保护需求，从而导致数据更易访问。

投资顾问应当考虑如何更新网络安全计划以应对这些技术的独特风险。就此而言，董事可能需要考虑以下问题：

- 投资顾问能否识别、检测和应对RPA和AI/ML带来的新兴威胁（包括加强安全开发实践）？
- 投资顾问将如何维护使用RPA和AI/ML（包括算法和模型）存储/处理的信息的机密性和完整性？
- IT专家是否已与负责业务连续性计划或灾难恢复计划的基金公司内部人员开展合作以确保服务的持续可用性？

云服务的安全性如何？

过去十年，云服务和云服务赋能技术的出现导致组织看待其业务的方式发生变化。云服务可以帮助投资顾问提高敏捷性、自动化程度和营销效率。数字化转型和云技术应用可能引发诸多网络风险，包括：

- 分散的云服务治理可能导致整个企业的云安全功能支离碎裂、业务驱动的云安全目标与集中治理方式相互矛盾、控制措施缺乏且与企业无法融合；
- 了解和管理云端数据风险和隐私问题可能极具挑战；存储在配置错误的云服务中的数据可能会暴露敏感信息并违反相关法规；
- 匆忙迁移至云端可能会对安全性造成损害，从而导致漏洞渗透到设计和代码中；
- 缺乏针对云资产的身份和访问管理以及在管理新用户和第三方访问需求方面存在漏洞；以及
- 冗余规划受限以及对云服务故障准备不足。

就云安全而言，董事可能需要考虑以下问题：

- 投资顾问是否确定了符合组织风险承受能力的云环境基本安全要求？
- 投资顾问是否确定了针对云服务的控制措施以及相关角色和职责以解决阻碍风险缓解工作的治理和技术问题？
- 投资顾问如何管理云平台和相关应用程序的用户身份？
- 投资顾问是否通过自动化建立了对安全事件或故障的快速响应能力？

远程工作带来虚拟环境风险

新冠疫情导致企业的短期和长期运营模式发生重大转变。如今，许多投资顾问都已经意识到远程工作模式带来的经济和运营优势。投资顾问应当确保员工拥有在虚拟办公环境中工作所需的设备、工作方法、访问权限和技术，尤其是在需要尽量减少接触以及业务和社区干扰的情况下。此外，内部威胁计划可能需要重新评估，因为许多组织将查看以前的工作行为模式，以此建立识别网络或应用程序异常活动的基本标准。远程劳动力的出现导致攻击面不断扩大，并且还会带来其他网络安全风险，包括：

- 员工可能使用未经安全组织充分审查或存在未识别/未修复漏洞的远程协作和数据共享工具。
- 员工可能通过远程协作和数据共享工具不恰当地共享/存储敏感信息。
- 远程员工可能会被诱骗通过网络钓鱼邮件或社交软件提供敏感信息。
- 远程访问基础设施可能缺乏容量，无法满足增加的使用量。
- 不当使用缺乏适当安全措施和监控机制的个人设备可能导致员工意外暴露敏感数据、故意窃取基金和股东数据并且增加犯罪分子破坏这些设备的风险。

董事会成员可能需要考虑以下问题：

- 投资顾问开展网络安全工作的总体方法能否在转向居家办公的过程中发挥作用？
- 投资顾问是否改进了组织的IT基础设施以管理不断增长的远程访问规模和网络流量？
- 投资顾问是否加强了组织的远程访问控制以便为持续或增加的内部网络远程访问提供适当的安全保障（例如MFA）？
- 投资顾问是否改进了现有内部威胁监控计划并加强了内部和第三方活动监控？
- 投资顾问是否提高了安全意识并加强了威胁检测和响应以促进对恶意活动的主动识别？
- 投资顾问是否拥有与远程使用公司发放硬件和员工个人电子设备相关的政策、控制措施和监控能力？
- 投资顾问是否根据从虚拟运营中吸取的经验教训调整了员工培训和政策？

总结

有效的网络安全计划始于对网络风险的适当治理。高级管理层应帮助董事会了解网络安全控制措施的设计和有效性，就基金网络风险的关键领域进行公开对话。因此，管理层应明确如何制定网络安全计划，并确保网络安全负责人具备降低网络事件发生概率所需的技能、资源和方法，以及在发生网络事件时检测和减轻任何潜在损害的能力。

董事会成员应继续探索如何将网络安全监督纳入整体风险监督工作。虽然网络安全正在迅速发展并且有时会表现出较高的技术复杂性，但是董事依然需要：

- 了解主要威胁的一般特征；
- 就如何减轻和管理风险与管理层展开对话；
- 了解如何识别网络风险和数据安全事件以及制定了哪些响应机制；
- 了解可能影响基金和网络安全计划监督的关键网络安全风险点。

与其他监督角色一样，董事有权针对网络安全相关问题作出商业判断。为此，董事会应当掌握适当的信息，并且根据机构所面临的风险提出适当的问题。为了提高董事会会议效率，高级管理层、技术主管和董事须就这些复杂的技术问题如何影响投资顾问、基金管理主体和第三方服务提供商的关键业务风险，如何识别这类问题以及围绕问题事件升级、沟通和报告机制等相关公司治理事项达成共识。

共同基金董事论坛网络安全监督工作组

Sameer Airyil，高级经理，Deloitte & Touche LLP

Colleen Brown，合伙人，Sidley Austin LLP

Krissy Davis，副主席，美国投资管理行业领导人，Deloitte & Touche LLP

Nathan Greene，合伙人，Sidley Austin LLP

Thomas Hayden，董事会主席，Oakmark Funds

Paul Kraft，合伙人，投资管理行业卓越品牌领导人，Deloitte & Touche LLP

Peg McLaughlin，董事，Manning and Napier Funds

Lloyd Wennlund，董事会主席，Datum One Series Trust；董事，Calamos Funds

Christopher Wilson，董事会主席，Invesco Funds

尾注

1. US Executive Office of the President, "Cost of malicious cyber activity to the US economy," Council of Economic Advisors, February 2018.
2. The impact of data breaches on reputation & share value: A study of US marketers, IT practitioners and consumers," Ponemon Institute LLC, May 2017.
3. https://gdpr-info.eu/issues/fines-penalties/
4. In re Caremark Int' l Deriv. Litig., 698 A.2d 959 (Del.Ch. 1996)
5. Firemen' s Retirement System of St. Louis v. Sorenson, et al., C.A. No. 2019-0965-LWW.
6. US Securities and Exchange Commission (SEC), IM Guidance Update, No. 2015-02, April 2015 ("IM Cybersecurity Guidance").
7. SEC, Cybersecurity and resiliency observations, Office of Compliance Inspections and Examinations, January 27, 2020 ("Cybersecurity Observations").
8. SEC, CF Disclosure Guidance: Topic No. 2 Cybersecurity, Division of Corporation Finance, October 13, 2011.
9. See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release Nos. 33-11028; 34-94197; IA-5969; IC-3449, February 2022. Available at https://www.sec.gov/rules/proposed/2022/33-11028.pdf. ("38a-2 Proposing Release")
10. Securities and Exchange Commission (SEC), "SEC proposes cybersecurity risk management rules and amendments for registered investment advisers and funds," press release 2022-20, February 9, 2022.
11. See Cybersecurity Observations.
12. See 38a-2 Proposing Release.
13. The SEC staff has recommended that advisers and funds understand the cybersecurity threats and vulnerabilities relevant to their businesses.
14. See IM Cybersecurity Guidance.
15. Ibid.
16. This focus on cybersecurity oversight from the perspective of correlating risk with specific business functions is discussed in Parenty, T. & Domet, J. Sizing up Your Cyberrisks. Harvard Business Review (2019).
17. See IM Cybersecurity Guidance at 2.
18. See IM Cybersecurity guidance. See also Cybersecurity Observations.
19. See IM Cybersecurity Guidance.
20. Ibid.
21. Ibid.
22. Ibid.
23. Ibid.
24. SEC, "SEC announces three actions charging deficient cybersecurity procedures," press release 2021-169, August 30, 2021.
25. See IM Cybersecurity Guidance.

报告原名*Cybersecurity and the evolving threat landscape: The role of the mutual fund director*由德勤美国与共同基金董事论坛联合撰写，德勤中国投资管理业团队进行翻译。

联系我们

我们的专业洞察可助您充分利用和发挥变革的优势。如您正在寻求行业切入点以应对挑战，敬请与我们联系。

郭新华
德勤中国金融服务业
投资管理业主管合伙人
电话：+86 10 8520 7289
电子邮件：jasonguo@deloitte.com.cn

曹樑
德勤中国金融服务业
财富管理咨询主管合伙人
电话：+86 21 2312 7154
电子邮件：hencao@deloitte.com.cn

薛梓源
德勤中国风险咨询
网络安全与战略风险事业群主管合伙人
电话：+86 10 8520 7315
电子邮件：tonxue@deloitte.com.cn

何晓明
德勤中国风险咨询
网络安全合伙人
电话：+86 10 8512 5312
电子邮件：the@deloitte.com.cn

蔡帼娅
德勤中国金融服务业
财富管理咨询总监
电话：+86 21 2316 6368
电子邮件：cycai@deloitte.com.cn

刘琪婷
德勤中国金融服务业
财富管理咨询总监
电话：+86 21 2312 7092
电子邮件：julietliu@deloitte.com.cn

杨婧
德勤中国金融服务业
审计及鉴证高级经理
电话：+86 10 8512 4461
电子邮件：jennygzyang@deloitte.com.cn

办事处地址

北京
北京市朝阳区针织路23号楼
国寿金融中心12层
邮政编码：100026
电话：+86 10 8520 7788
传真：+86 10 6508 8781

长沙
长沙市开福区芙蓉北路一段109号
华创国际广场3号栋20楼
邮政编码：410008
电话：+86 731 8522 8790
传真：+86 731 8522 8230

成都
成都市高新区交子大道365号
中海国际中心F座17层
邮政编码：610041
电话：+86 28 6789 8188
传真：+86 28 6317 3500

重庆
重庆市渝中区民族路188号
环球金融中心43层
邮政编码：400010
电话：+86 23 8823 1888
传真：+86 23 8857 0978

大连
大连市中山路147号
申贸大厦15楼
邮政编码：116011
电话：+86 411 8371 2888
传真：+86 411 8360 3297

广州
广州市珠江东路28号
越秀金融大厦26楼
邮政编码：510623
电话：+86 20 8396 9228
传真：+86 20 3888 0121

杭州
杭州市上城区飞云江路9号
赞成中心东楼1206室
邮政编码：310008
电话：+86 571 8972 7688
传真：+86 571 8779 7915

哈尔滨
哈尔滨市南岗区长江路368号
开发区管理大厦1618室
邮政编码：150090
电话：+86 451 8586 0060
传真：+86 451 8586 0056

合肥
安徽省合肥市蜀山区潜山路111号
华润大厦A座1506单元
邮政编码：230022
电话：+86 551 6585 5927
传真：+86 551 6585 5687

香港
香港金钟道88号
太古广场一座35楼
电话：+852 2852 1600
传真：+852 2541 1911

济南
济南市市中区二环南路6636号
中海广场28层2802-2804单元
邮政编码：250000
电话：+86 531 8973 5800
传真：+86 531 8973 5811

澳门
澳门殷皇子大马路43-53A号
澳门广场19楼H-L座
电话：+853 2871 2998
传真：+853 2871 3033

南昌
南昌市红谷滩区绿茵路129号
联发广场写字楼41层08-09室
邮政编码：330038
电话：+86 791 8387 1177

南京
南京市建邺区江东中路347号
国金中心办公楼一期40层
邮政编码：210019
电话：+86 25 5790 8880
传真：+86 25 8691 8776

宁波
宁波市海曙区和义路168号
万豪中心1702室
邮政编码: 315000
电话：+86 574 8768 3928
传真：+86 574 8707 4131

三亚
海南省三亚市吉阳区新风街279号
蓝海华庭 (三亚华夏保险中心) 16层
邮政编码：572099
电话：+86 898 8861 5558
传真：+86 898 8861 0723

上海
上海市延安东路222号
外滩中心30楼
邮政编码：200002
电话：+86 21 6141 8888
传真：+86 21 6335 0003

沈阳
沈阳市沈河区青年大街1-1号
沈阳市府恒隆广场办公楼1座
3605-3606单元
邮政编码：110063
电话：+86 24 6785 4068
传真：+86 24 6785 4067

深圳
深圳市深南东路5001号
华润大厦9楼
邮政编码：518010
电话：+86 755 8246 3255
传真：+86 755 8246 3186

苏州
苏州市工业园区苏绣路58号
苏州中心广场58幢A座24层
邮政编码：215021
电话: +86 512 6289 1238
传真: +86 512 6762 3338 / 3318

天津
天津市和平区南京路183号
天津世纪都会商厦45层
邮政编码：300051
电话：+86 22 2320 6688
传真：+86 22 8312 6099

武汉
武汉市江汉区建设大道568号
新世界国贸大厦49层01室
邮政编码：430000
电话：+86 27 8538 2222
传真：+86 27 8526 7032

厦门
厦门市思明区鹭江道8号
国际银 361001
电话：+86 592 2107 298
传真：+86 592 2107 259

西安
西安市高新区唐延路11号
西安国寿金融中心3003单元
邮政编码：710075
电话：+86 29 8114 0201
传真：+86 29 8114 0205

郑州
郑州市金水东路51号
楷林中心8座5A10
邮政编码：450018
电话：+86 371 8897 3700
传真：+86 371 8897 3710

关于德勤

德勤中国是一家立足本土、连接全球的综合性专业服务机构，由德勤中国的合伙人共同拥有，始终服务于中国改革开放和经济建设的前沿。我们的办公室遍布中国30个城市，现有超过2万名专业人士，向客户提供审计及鉴证、管理咨询、财务咨询、风险咨询、税务与商务咨询等全球领先的一站式专业服务。

我们诚信为本，坚守质量，勇于创新，以卓越的专业能力、丰富的行业洞察和智慧的技术解决方案，助力各行各业的客户与合作伙伴把握机遇，应对挑战，实现世界一流的高质量发展目标。

德勤品牌始于1845年，其中文名称“德勤”于1978年起用，寓意“敬德修业，业精于勤”。德勤专业网络的成员机构遍布150多个国家或地区，以“因我不同，成就不凡”为宗旨，为资本市场增强公众信任，为客户转型升级赋能，为更繁荣的经济、更公平的社会和可持续的世界而开拓前行。

Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成员所网络和它们的关联机构（统称为“德勤组织”）。德勤有限公司（又称“德勤全球”）及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为承担责任，而对相互的行为不承担任何法律责任。德勤有限公司并不向客户提供服务。

德勤亚太有限公司（即一家担保有限公司）是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体，在亚太地区超过100座城市提供专业服务。

请参阅http://www.deloitte.com/cn/about了解更多信息。

本通讯中所含内容乃一般性信息，任何德勤有限公司、其全球成员所网络或它们的关联机构（统称为“德勤组织”）并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合资格的专业顾问。

我们并未对本通讯所含信息的准确性或完整性作出任何（明示或暗示）陈述、保证或承诺。任何德勤有限公司、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。德勤有限公司及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体。

Designed by CoRe Creative Services. RITM1172445.

这是环保纸印刷品