protiviti®
Global Business Consulting
甫瀚

SEC 网络安全披露升级：努力提振投资者信心

2023年8月

2023年7月26日，美国证券交易委员会 (SEC) 根据《1934年证券交易法》的报告要求，通过了上市公司网络安全风险管理、战略、治理和异常事件报告相关规则的修正案[1]。SEC认为，网络安全威胁和异常事件对上市公司、投资者和市场参与者构成了持续的风险，依据是网络犯罪分子使用日益复杂的方法发动了更加密集的攻击。

修正案旨在就如下方面为投资者提供更好的信息和透明度：网络安全风险和威胁、公司识别和管理威胁的能力、以及高级管理层和董事会提供的监督和治理。修正案的目的是让投资者更好地管理投资组合中的风险，因为网络安全事件可能对公司的运营和业绩产生重大影响。

概述

已通过的修正案增加了在 SEC 注册的公司的报告和披露要求。新要求可归纳如下：

关键定义

根据自 2022 年 3 月提出拟议规则以来收到的评论意见，SEC 调整了修正案的原始措辞，将一些关键术语纳入其中。了解这些最终版关键术语的含义对于公司确定披露内容非常重要。

- **重要性：** SEC 在许多要求中强调了重要性的概念。就修正案而言，“重要性” 将根据司法判决中确立的先例进行评估,例如,如果在做出投资决策时“很有可能一个合理的股东会认为该信息很重要”，或者该信息会 “极大地改变可获得信息的 ‘总体组合’ ”，那么该信息就是重要的。此外，对相关信息 “重要性质的怀疑” 应 “以有利于投资者的方式解决”。[2] 评估重要性需要考虑定量和定性因素，如公司历史或未来的财务状况或运营情况、公司声誉和品牌形象、客户或供应商关系，以及是否符合法规等。分析应考虑到所有事实和情况，既涉及直接后果，也涉及任何长期影响。

- **网络安全事件：** SEC 使用的定义与 NIST SP 800-137 和《2022 年关键基础设施网络事件报告法》（CIRCIA）中阐述的网络安全事件定义基本一致。这三个定义都侧重于信息系统的保密性、完整性和可用性。SEC 定义明确指出，网络安全事件是 “在注册人信息系统上发生的或通过注册人信息系统进行的一项未经授权事件，或一系列相关事件，危及其信息系统或其中任何信息的保密性、完整性或可用性”。SEC 对拟议版本的修订是将 “一系列相关的未经授权事件” 纳入作为定义的一部分。此外，根据评论意见，SEC 放弃了披露 “一系列先前未披露的单独不重要的网络安全事件在汇总后变得重要” 的要求。

网络安全事件报告

网络安全事件报告的重点与 2022 年 3 月的拟议版本略有不同。报告应审查重大网络安全事件的影响，而不需要报告事件细节。报告的重要方面包括以下内容：

[1] “网络安全风险管理、战略、治理和异常事件披露”，美国证券交易委员会，2023 年 7 月 31 日，www.sec.gov/files/rules/final/2023/33-11216.pdf。

[2] TSC 工业公司诉北路公司，参见 “美国最高法院判例汇编” 第 426 卷，第 438 页 (1976) 一案。

- 报告应侧重于任何被确定为重要事件的性质、范围和时间，及其影响或合理可能的影响。
- 应在确定事件已造成或可能造成重大影响后的四个工作日内通过 8-K（或外国私人发行人 6-K 表）进行报告。
- 如果第三方服务提供商或供应商发生的网络安全事件被认为具有重大影响，则报告应包括这些事件。
- 如果网络安全事件的影响或事实发生变化，公司可以通过提交更新的 8-K/6-K 表或定期报告（10-Q 或 10-K）来更新报告。

描述风险管理流程

最初提出修订 S-K 条例，是因为 SEC 发现，许多之前披露过网络安全事件的公司没有提供足够的有关其网络安全风险监督或流程的信息。根据新的修正案，SEC 正在采取一种更具规范性的方法，要求公司描述其识别、评估和管理重大网络安全风险和威胁的流程。具体要求包括：

- 网络安全风险管理职能的概括描述，包括如何识别风险、以及用于评估风险水平和管理措施以确保风险被降低至并维持在合理水平的流程；
- 网络安全风险管理职能如何整合到更广泛的企业风险管理体系和流程中的见解，例如，与企业风险管理流程结合使用的网络安全风险报告和监测流程；
- 关于发行人是否聘请评估师、顾问、审计师和其他第三方以协助其网络安全风险管理职能和流程的披露；
- 用于监督和识别与使用第三方服务提供商有关的网络安全风险的流程的描述；
- 来自网络安全威胁的任何风险，包括与以往事件相关的风险，是否对公司的业务战略、运营或财务状况造成重大影响，或是否有合理的可能造成重大影响，如果是，如何造成影响。

董事会和管理层的治理作用的披露

S-K 条例的修正案还包括与治理有关的新要求。董事会的监督，以及管理层在评估和管理网络安全风险方面的角色需要披露。披露的主要内容包括：

- 负责监督自网络安全威胁产生的风险的董事会或下属委员会；
- 董事会或下属委员会了解网络安全风险的流程，例如，董事会获得信息的频率，以及董事会在监督网络安全风险方面的角色和责任；
- 负责评估和管理网络安全风险的管理职位或委员会，包括这些职位所涉人员的相关专业知识；
- 管理层或下属委员会用以了解和监控网络安全事件的预防、检测、缓解和补救的流程；
- 管理层是否向董事会或下属委员会报告有关网络安全风险的信息。

需注意 SEC 选择删除了拟议版本中有关董事会成员的网络安全专业知识的披露要求。许多评论者指出，这方面的人才储备有限，而且由于资源有限，规模较小的公司将处于不利地位。

外国私人发行人

修正案承认投资者需要外国私人发行人提供有关网络安全实践和事件的类似信息。修正案明确规定外国私人发行人应通过表格 6-K 和表格 20-F 备案来提供此信息。

执行时间线

修正案确立了以下生效日期：

2023 年 12 月 15 日	在此日期或之后披露的 10-K 和 20-F，适用于本修订案
2023 年 12 月 18 日或联邦公报发布日期后 90 天，以较晚者为准	8-K 和 6-K 披露从此日期开始
2024 年 6 月 15 日或联邦公报发布日期后 270 天，以较晚者为准	对于“小企业”，8-K 和 6-K 披露从此日期开始

对于 SEC 来说，这些生效日期异常紧迫，适用于申报日期为“在此日期或之后”的年度报告以及其他所需定期报告。需要注意的是，属于“小企业”类别的组织在需要遵守 8-K 或 6-K 表格中概述的规则之前，可额外获得 180 天的时间。但是，这些公司必须在 12 月满足 10-K 和 20-F 披露的报告要求。一般来说，如果一家公司的公众持股量少于 2.5 亿美元，或年收入少于 1 亿美元的同时没有公众持股量或公众持股量少于 7 亿美元，则该公司符合“小企业”的条件。

为变革做好准备 — 需要考虑的几个要点

在为合规做准备时，发行人应开始让相关业务负责人熟悉新要求。企业至少应让其网络安全、法律、隐私和合规团队参与这些初步讨论。

首先要考虑的是新法规的近期时间表。根据公司的财政年度结束时间，年度报告要求（通过 10-K 和 20-F 披露）和任何安全事件报告（通过 8-K 和 6-K 披露）将于 2023 年 12 月或之后开始。发行人在为这些关键日期做准备时，应了解和制定针对不同类型的申报文件，所涵盖的叙述深度和范围。

在准备过程中,我们鼓励各组织审视其事件响应计划,并从确保其符合 SEC 强调的以下关键定义开始。在这方面达成一致可能会对事件响应计划的启动时间和方式产生深远影响。

- **网络安全事件**是指在注册人的信息系统上发生的或通过注册人的信息系统进行的一项未经授权的事件或一系列相关的未经授权的事件，这些事件危及注册人的信息系统或其中保存的任何信息的保密性、完整性或可用性。

- **网络安全威胁**是指在注册人的信息系统上发生或通过注册人的信息系统进行的任何潜 在的未经授权的事件，该事件可能对注册人的信息系统或其中保存的任何信息的保密性、完整性或可用性造成不利影响。

- **信息系统**是指注册人拥有或使用的电子信息资源，包括由该信息资源控制的物理或虚拟基础设施或其组成部分，旨在为收集、处理、维护、使用、共享、传播或销毁注册人的信息，以维持或支持其运营。

组织特别关注的是报告事件的四个工作日窗口。上市公司需要在四个工作日内提交 Form 8-K 文件，这通常与注册人有被提前通知和有时间去提前准备披露草案的交易和事件有关。然而，对于这一规定，一旦突发的安全事件在性质上被评估具有重要性，窗口就开始了。因此，组织需要确保他们牢牢掌握识别和升级报告事件的流程，并在关键时刻发生时定义重要性，因为 SEC 的修正案要求决策“不得无故拖延”。由于这一过程需要收集与事件的性质、范围和时间相关的必要信息，并让相关方做出判断，因此提前计划其运作方式、考虑的标准以及由谁担任是有意义的。此外，需要持续获取适当的数据，因为可能需要通过 8-K/6-K 表格或其他计划的定期申报文件提供持续更新。这些要点应纳入事件响应计划中。

尽管重要性对于许多组织来说可能是一个“不断变化的目标”，但实际上，SEC 决定不制定网络安全的具体门槛，因为这样做将严重偏离其在该主题上的政策。因此，SEC 恢复了在证券法中处理重要性的案件中规定的长期标准，例如“合理的投资者”测试。这使得该决定成为一个法律问题，并强烈指出在确定重要性时需要让法律顾问参与决策过程。

当然，对导致或可能导致组织的流动性或财务状况发生变化，资本资源的组合和相对成本发生变化，或对持续性收入或收益产生不利影响的已知趋势或不确定因素进行分析，将对重要性的确定产生影响。

在某些情况下，事件可能对国家安全或公共安全构成重大风险（由美国司法部长确定）。在这些情况下，在书面通知 SEC 后，可以准予延迟 8-K/6-K 表披露（30 至 60 天，视具体情况而定）。出现这种情况的可能性表明，组织在其事件响应计划中制定了根据情况通知相关联邦执法机构并与其进行协调的规定。

第三方在所有行业的关键业务流程中继续发挥着不断扩大的作用。这个话题引起了很多评论者对 SEC 的反馈。尽管该法规承认第三方服务提供商的作用和影响，但最终规则陷入了灰色地带。SEC 明确表示：“我们没有豁免注册人披露其使用的第三方系统上的网络安全事件，也没有为披露的第三方系统信息提供安全港。”

根据发生在第三方系统上的事件的具体情况，服务提供商及其客户可能都需要披露，或只要求其中一方披露，另一方不要求披露，或两者都不要求披露。这将是一个挑战，因为公司对无法控制的第三方系统的可见性通常不足。好消息是，最终规则承认了这些挑战的存在，规定注册人应根据其已知或合理可用的信息披露第三方系统问题，并且符合 SEC 关于披露难以获得的信息的一般规则。

为此，最终规则一般不要求注册人根据其合同义务和权利以及注册人的披露控制和程序，在与第三方服务提供商的常规沟通渠道之外进行额外的问询。底线：组织需要意识到第三方在其业务运营中发挥的重要性，并且如果源自第三方的事件对其运营产生重大影响，应准备好回应投资者的问题。在服务合同中加入一项条款，明确第三方对注册人披露的义务，并确保适当考虑和评估第三方的使用和第三方风险，作为整体网络安全风险管理的一部分，这也可能是一个明智之举。

在确定表格 10-K 和 20-F 中网络安全管理措施的适当详细程度时（特别关注风险管理、战略和治理），一个良好的出发点可能是发行人的环境、社会和治理（ESG）报告。一些组织已经在该报告中概述了他们的网络安全和隐私管理措施。另一种方式，查看同行业其他组织的 ESG 报告和过去的网络安全披露，以确定他们使用了多少细节来描述其管理措施，可能会有所帮助。

准备改变 — 如果从零开始

对于从零开始的公司，可以考虑以下几个重要问题，从而找到解决方式：

- **有哪些流程（如果有）用于评估、识别和管理网络安全威胁带来的重大风险？**
  - 这些流程的描述是否足够详细，以使一位合理的投资者能理解？
  - 是否有适当的流程来监督和识别与任何第三方服务提供商相关的网络安全威胁所带来的重大风险？
  - 如何将描述的网络安全流程融入到整体风险管理体系或流程中？
  - 公司是否在其流程中使用评估师、顾问、审计师或其他第三方？

- **网络安全威胁（包括以前的任何网络安全事件）带来的任何风险是否对公司的业务战略、运营业绩或财务状况产生重大影响（或相当可能产生重大影响）？如果是这样，怎么办？**
  - 网络安全风险是否被视为注册人战略制定、财务规划和资本分配流程的一部分？如果是，以怎样方式实现？
  - 管理层在评估和管理网络安全威胁的重大风险方面的作用是什么？
- **董事会如何监督网络安全威胁带来的风险？**
  - 是否有董事会或下属委员会负责此类监督？
  - 董事会或下属委员会了解这些风险的流程是什么？
- **哪些管理职位或委员会负责评估和管理网络安全风险？**
  - 这些人员的相关专业知识是怎样的？
  - 这些人员或委员会了解并能够监控网络安全事件的预防、检测、缓解和补救的流程是什么？
  - 这些人员或委员会如何向董事会或其下属委员会报告有关网络安全风险的信息？

总结

在通过这些修正案时，SEC 试图找到共同点，以避免使公司遭受安全风险并保护投资者的利益。但其规定性的做法并非没有争议。正如两位持不同意见的 SEC 委员之一所言，最终规则在 2018 年 2 月 SEC 发布的释义文件中“强制地规定了一个披露体制”，其中讨论了公司在根据证券法准备申报文件时应如何考虑网络安全风险和事件的重要性。用他的话说，修正案“对现行制度进行了重击，并为网络安全事项设立了其他任何主题上都不存在的新披露义务。”[3]

也就是说，SEC 根据《1934 年证券交易法》的报告要求，对上市公司网络安全风险管理、战略、治理和事件报告规则进行了修订，旨在帮助确保网络安全风险和事件信息及时性和一致性。通过数字技术和电子通信进行的世界经济活动数量显著且日益增加，这进一步突显了这些修正案的重要性。投资者和其他资本市场参与者依赖于公司使用安全可靠的信息系统和数据来开展业务。随着威胁形势的不断发展，网络安全继续吸引着投资者的兴趣和监管机构的审查。这种审查不仅会针对上市公司，还会针对那些寻求上市的公司和被上市公司收购的公司。时间会证明这些新的披露是否符合他们的利益。

关于甫瀚 SOX 合规咨询和网络安全服务

甫瀚是国内最早为客户提供《萨班斯 – 奥克斯利法案》SOX404 合规咨询的专业机构之一，2004 年第一批需要 SOX 合规的 4 家企业，甫瀚为其中 3 家提供了咨询服务。截至 2022 年底，甫瀚已成功为超过 100 个客户提供 SOX404 合规咨询项目，得到市场与客户的高度认可。经过多年的积累与沉淀，甫瀚拥有一支技术过硬、经验丰富的 SOX 咨询团队，深入理解 SOX404 法案相关知识及 SEC 对于企业内部控制的期望和要求，合理准确地把控合规要点，有力支持企业的上市合规工作。

甫瀚可以为企业提供专业的网络安全服务，协助企业识别、防护、发现、响应网络安全事件，以增强企业管理网络安全事件的能力，减少安全事件为企业带来的影响。包括网络安全事件防护检测机制的规划和设计、网络安全事件监控响应的托管服务、网络安全平台及管理流程的评估和优化，以及协助企业进行网络安全事件的相关合规工作。

[3] “最终规则的声明：网络安全风险管理、战略、治理和异常事件披露”，专员 Mark T.Uyeda，2023 年 7 月 26 日，www.sec.gov/news/statement/uyeda-statement-cybersecurity-072623。

关于甫瀚咨询

甫瀚咨询是一家全球性的咨询机构，为企业带来领先的专业知识、客观的见解、量身定制的方案和卓越的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球超过25个国家的逾85家分支机构和成员公司，我们为客户提供财务、信息技术、运营、数据、数字化、环境、社会及管治、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询荣膺2023年《财富》杂志年度最佳雇主百强，我们为超过80%的财富100强及近80%的财富500强企业提供咨询服务，亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。甫瀚咨询是Robert Half International Inc.（纽约证券交易所代码：RHI）的全资子公司。RHI于1948年成立，为标准普尔500指数的成员公司。

联系我们

李莹
联席董事，SOX 合规咨询业务联络人
Jessica.Li@protiviti.com

彭銘楷
董事总经理，网络安全咨询业务联络人
Michael.Pang@protiviti.com

余达丽
项目总监，网络安全咨询业务联络人
Angela.Yu@protiviti.com

公司地址

北京
朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话：(86.10) 8515 1233

上海
徐汇区陕西南路 288 号
环贸广场二期 1915-16 室
电话：(86.21) 5153 6900

深圳
福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话：(86.755) 2598 2086

香港
中环 干诺道中 41 号
盈置大厦 9 楼
电话：(852) 2238 0499

protiviti 甫瀚