全球观点与视角

网络安全 2022

第一部分：SEC 新提案如何能够改变现状

第二部分：关键的伙伴——内部审计和首席信息安全官（CISO）

第三部分：网络事件的应对和恢复

The Institute of Internal Auditors

目录

第一部分

美国证券交易委员会（SEC）的新议案将如何改变这场游戏

专家简介

Andy Watkin-Child

Watkin-Child 拥有 20 年的网络安全、风险管理和技术方面的从业经验，是 Augusta 集团（一家网络安全和网络风险管理、监督和确认相关问题解决方案提供商）的创始人之一。他曾在网络安全、网络风险管理、运营风险和技术相关的第一、第二道防线（LoD）领域担任国际领导职务，并与涉及工程与制造、金融服务以及出版和传媒等领域，资产负债表超过 1 万亿欧元的公司领导团队展开合作。他是管理委员会、全球风险领导者团队以及网络安全、运营风险和《通用数据保护条例》（GDPR）委员会中经验丰富的成员。

Manoj Satnaliwala

Satnaliwala 是美国房屋抵押贷款供应商 Caliber Home Loans 的首席审计执行官兼内部审计高级副总裁，负责公司所有的审计工作，与审计委员会直接互动。在此之前，他曾在瑞迪安集团（美国第三大上市抵押贷款保险公司）担任审计职能部门领导，还在普华永道会计师事务所担任内部审计总监，在普华永道会计师事务所任职期间，他曾为一家大型银行控股企业管理 CCAR 项目中的内部审计控制措施。

简介

新监管提案将产生巨大影响

2022 年新周期，或是过去的几年中，全球整体形势不容乐观，也在一系列复杂交错的因素影响下，网络风险情况也日益严峻。乌克兰危机爆发、新冠肺炎疫情持续以及世界重要经济体之间的关系日益紧张，在这些不确定性因素的共同作用下，网络安全已然成为内部审计人员风险版图中至关重要的一环。

然而，今年以来网络安全相关领域持续发展，必将对各个领域的组织产生广泛影响，内部审计人员要投入更多的时间和精力去理解和掌控相关情况。其中最重要的内容是美国证券交易委员会提出的两项新监管提案，其中第二项提案尤其值得注意，因为此项提案要求在美经营的上市企业就组织网络安全政策、流程、治理战略以及董事会对网络安全的知识和经验（如有）进行披露。提案一旦生效（可能会以某种形式实施），上市企业，无论所属行业和规模大小，都必须遵守新规。毫不夸张地讲，这将开启网络安全的新篇章，并成为内部审计职业新的课题，内部审计也将在驾驭组织应对此项挑战中发挥关键性作用。

虽然应对此项挑战绝非易事，但内部审计已经掌握了为这项不断发展的风险领域提供确认服务所需的工具和技能。国际内部审计师协会（IIA）发布的有关网络安全的全球知识系列概要包含三部分内容，其中第一部分将概述 SEC 的新提案，其中包括新提案对美国以及全球网络安全报告监管的影响。还就新规生效后，内部审计人员如何在帮助组织管理新的合规环境中发挥重要作用进行探讨。

做好准备

网络安全在风险版图中占据主导地位

当今时代最重要的风险类型

2022 年所有行业、各个层级的组织都将网络安全视为首要考虑的问题，IIA《2022 年北美内部审计脉搏动态报告》[1]中的数据清楚地反映了这一点。当被问及如何对组织面临的 13 项主要风险进行评级时，受访的内部审计领导者们将技术相关的风险排在了所有风险种类的前三位，分别是网络安全、信息技术和第三方关系（通常包含信息技术服务）。在这三项风险中，网络安全排在第一位，85%的受访者将其视为高风险或超高风险，比排名第二位的信息技术风险高 24%。

这样的担忧并非空穴来风。2021 年，几乎所有种类的网络攻击案例都以惊人的速度在不断增长。《2022SonicWall 网络安全报告》[2]数据显示，2021 年加密型网络威胁数量增长 167%（1040 万次攻击），勒索病毒增长 105%（6.233 亿次攻击），非法加密挖矿（通过攻击计算机来挖掘加密货币）增长 19%（9710 万次攻击），入侵企图增长 11%（5.3 万亿次攻击），直接针对物联网（IoT）的恶意软件增长 6%（6010 万次攻击）。

此外，所有攻击都伴随着巨大的损失和代价。思科/网络安全风险投资公司《2022 年网络安全年鉴》[3]中数据显示，到 2025 年，网络攻击每年造成的损失将达到 10.5 万亿美元，年均增长率为 15%。

而且，以上情况尚且未将地缘政治相关的巨大变革对网络安全的影响纳入考虑之中。即便是在俄乌冲突爆发之前，就有充足的证据表明，高级网络攻击影响力和发生频率正在不断增加。2020 年德克萨斯州 SolarWind 系统在某黑客团队攻击下遭到破坏，导致覆盖超 18,000 用户[4]——其中包括微软、思科、因特尔、德勤、五角大楼部分部门、美国国土安全部、能源局以及国家核安全局——的数字基础设施在长达数月的时间里发生数据泄露且未能发现。

2021 年美国科洛尼尔管道运输公司疑似遭到网络攻击[5]。此次攻击事件造成近半成向东海岸运输的油气管道暂时中止。最终，科洛尼尔向黑客团队 DarkSide 支付将近 500 万美元赎金，才最终得以重启网络系统，并恢复相关数据。

[1]. 国际内部审计师协会（IIA），《2022 北美内部审计脉搏动态报告》，2022 年 3 月 https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of-internal-audit/

[2]. SonicWall，《2022 SonicWall 网络威胁报告》，2022 年，https://www.sonicwall.com/2022-cyber-threat-report/.

[3]. Steve Morgan,《2022 网络安全年鉴：100 项事实、图表、预测和数据》，网络安全风险投资公司、思科，2022 年 1 月 19 日，https://cybersecurityventures.com/cybersecurity-almanac-2022/.

[4]. Isabella Jibilian and Katie Canales, “美国已经做好准备对俄罗斯就 SolarWinds 网络攻击进行制裁。下文将简要阐述大规模攻击发生的原因及其重要意义。”商业知情人士，2021 年 4 月 15 日更新， https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[5]. Andrew Marquardt,“拜登警告俄罗斯网络攻击后续。下文将讲述去年一条主要的石油网线遭到攻击后发生了什么”《财富》，2022 年 3 月 22 日， https://fortune.com/2022/03/22/biden-warns-russian-cyber-attack-pipeline/.

巨大改变

迈向网络事件披露的历史性第一步

相关提案

美国证券交易委员会（SEC）在两个月之内发布了两项期待已久的提案，其内容主要针对商业领域的网络安全问题。第一项提案[6]于 2022 年 2 月发布，主要涉及注册投资顾问公司、注册投资公司以及商业发展公司或基金公司。提案中规定，顾问公司和基金公司必须做到：

- 为应对可能会损害咨询客户和资金投资方利益的网络安全风险制定正式的政策和流程，并将其落到实处。
- 以一种新型保密形式向 SEC 报告影响顾问或其基金或私募基金客户的重大网络安全事件。
- 公开披露过去两个财年组织简介和上市登记表中出现的网络安全风险和重大网络安全事件。

另外，此项提案将为顾问和基金公司设置前所未有的要求，从而提升网络安全相关信息的可获取度，同时协助提升 SEC 的监管和执行能力。

“网络风险与 SEC 的三项使命，尤其是与我们保护投资方利益并维护市场秩序的目标息息相关，”SEC 主席 Gary Gensler 在新闻发布会[7]上说，“SEC 希望通过提案中的条款和修订内容来加强应对网络安全问题的准备程度，提升投资方对顾问和基金公司在应对网络安全威胁和攻击能力方面的信心。”

如果说以上这些条款尚未明确监管部门应该如何管理网络安全风险并报告网络安全事件，那么第二项提案则清晰地指出了 SEC 在这些方面的期待。第二项提案[8]于 2022 年 3 月正式发布，直接针对所有公开上市企业，提出要“严格遵循 1934 年《证券交易法》的报告要求，强化并规范有关上市公司网络安全风险管理、战略、组织治理和网络安全事件报告的披露工作。”为此，新规要求上市企业对以下内容进行披露：

- 公司在确定和管理网络安全风险方面的政策和流程。新规要求提交一份详尽但并不全面的的风险管理战略、政策和流程清单，具体内容有：
    - 注册企业是否拥有网络安全风险评估程序。
    - 注册企业是否外聘了与网络安全风险评估项目有关的评估人员、顾问、审计人员或其他第三方。
    - 注册企业是否制定了相应的政策和流程，就其第三方服务提供商相关的网络安全风险进行监督和确认。
    - 注册企业是否采取实际措施来预防和发现网络安全事件，并尽量降低其负面影响。
    - 注册企业是否具备应对网络安全事件的业务连续、应急和恢复预案。
    - 注册企业是否能够根据之前发生的网络安全事件对组织治理、政策、流程或技术进行相应的改革。

6. 美国证券交易委员会（SEC），《投资顾问公司、注册投资公司和商业发展公司的网络风险管理》，2022 年 2 月 9 日，https://www.sec.gov/rules/proposed/2022/33-11028.pdf.
7. 美国证券交易委员会（SEC），《SEC 有关注册投资顾问和基金公司的网络安全风险管理条例和修订案》，新闻发布会，2022 年 2 月 9 日， https://www.sec.gov/news/press-release/2022-20.
8. 美国证券交易委员会（SEC），《网络安全风险管理、战略、组织治理和事件披露》，2022 年 3 月 9 日 https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

- 网络安全相关的风险和事件是否已经或即将对注册企业的运营或财务状况产生影响。
- 注册企业是否将网络安全风险视为企业商业战略、财务规划以及资本分配的范畴之中。

- 管理层在执行网络安全政策和流程中发挥的作用，其中包括：
  - 是否指定某些管理岗位或委员会负责网络安全风险的衡量和管理工作。
  - 注册企业是否配备首席信息安全官或其他同等职能岗位。
  - 上述人员或委员会是否会向董事会或董事会下设网络安全风险委员会报告，以及多长时间报告一次。
  - 是否由董事会、董事会特定成员或董事会下设委员会对网络安全风险监督工作负责。
  - 董事会是否了解企业网络安全风险情况，多长时间会对网络安全风险进行一次讨论。
  - 董事会或董事会下设委员会是否以及如何将网络安全风险纳入企业商业战略、风险管理和财务监督之中。

- 董事会在网络安全方面的专业知识（如果有的话），以及董事会对网络安全风险的监督。其中包含的信息有：
  - 董事会是否具备网络安全领域的工作经验。
  - 董事会是否已经获取了网络安全方面的资格认证或教育背景。
  - 董事会是否具备有关网络安全的相关知识、技能或其他背景知识。

除此以外，提案中还包括一项修订案，需要填写表格 8-K，要求上市企业按照要求，像对待其他规划外的事件一样，在四个工作日之内就网络安全事件进行披露。需要披露的信息有：

- 发现事件的时间，以及事件是否仍在继续发展。
- 对事件性质和范围的简要描述。
- 数据是否遭到盗窃、变更、获取或被用于其他未经授权的事项。
- 网络安全事件对企业运营的影响。
- 企业是否已经或正在就事件造成的影响进行修复。

SEC 表示，这些披露内容将为投资方提供“连贯的、具有可比性的、有助于决策的”信息。Gensler[9]说：“如今，网络安全风险重要性逐步显现，成为上市企业必须应对的问题，未来，各个网络之间的联系会更加紧密，预测性数据分析的使用以及对数据不知满足的渴求也定会不断加剧，从而给我们的财务账目、投资项目和保密信息带来风险。因此，投资方希望了解更多有关上市企业如何管理这些风险的信息。”

[9]. Gary Gensler，《有关强制性网络安全披露提案的声明》，美国证券交易委员会（SEC），2022 年 3 月 9 日 https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

历史性的重要意义

上述规定条款的结构从很多方面与其他领域相关的 SEC 披露条款大体相似，其中包括财务状况和运营结果（《萨班斯·奥克斯利法案》）、内部信息以及组织优势、劣势、机遇和威胁。然而，在此基础之上，通过强制要求对相关情况进行披露的方式，进一步提升对网络安全风险的重视程度，是前所未有的举动。

Watkin-Child 还就新规如何在其他国家和地区掀起巨大波澜进行了阐述："乌克兰危机证实了网络安全是一种武器，从 2016 年起，北约就开始将其纳入运作考虑之中，网络安全的攻击效力仅次于核武器，因为网络安全是一个运作的范畴，是国家基础设施的巨大威胁。SEC 的提案首先指向最大的参与者——贸易企业，但在我看来，由于全球的商业环境和政治环境错综复杂，未来还有可能会针对 SEC 权限以外的组织提出相应的要求。"

Watkin-Child 指出，在战争中，我们不能在一支单独军队的范畴下考虑网络安全问题；如果联盟关系脆弱，会直接影响整个联合行动。网络安全保护对于所有的上市和私营企业来说毫无二致。他说："如果美国的武器系统能够抵御非法侵入，但英国的系统遭到攻击，那么保护措施也毫无意义。因此，美国总统与北约在讨论其他事项以外，单独就建立统一的网络安全标准进行了商讨。我们必须这样做，因为如果商业机构收到利用，被用于攻击我们的电力系统，我们的水、电力、燃气以及医疗都将会受到毁灭性打击。"

诸如此类的潜在后果影响范围显然十分庞大，但同时我们也不能低估了组织层面的影响。而且虽然有很多因素都会影响网络安全的披露工作，但并不代表所有因素带来的结果都是负面的。

Watkin-Child 说："披露还涉及到合法合规的问题，但是正如提案中所陈述的，上市公司不仅要向 SEC 报告，还要向可能会影响组织业务的所有市场参与方报告。投资方群体、信用评级机构、保险公司会和 SEC 一起检验企业在网络安全方面的应对能力。披露工作会提升组织的透明度，虽然会伴随着一定的风险，但同时也会带来发展的机遇。"

内部审计的职责始终如一

确认、评估、交流

现有的各项工具

为帮助内部审计协助组织增加价值，2002 版《萨班斯·奥克斯利法案》（SOX）规定了内部审计职能需要承担的其他职责，同时为其解锁了新的发展机遇。的确，正如组织要适应新的法律规定，内部审计也要遵循 SOX 的相关规定。从 SEC 新提案的性质来看，网络安全领域也很可能出现相同的情况。

乍看之下，网络安全领域问题错综复杂，上述情况短期之内恐怕难以实现。《2022 年北美内部审计脉搏动态报告》[10]的受访者认为，网络安全在上市公司的审计计划中平均占比为 9%，较之前三年占比（7%）有所提升，但依然远低于财务报告占比（35%）。这是由多种因素导致的，其中包括预算限制、资源不足以及缺乏知识或经验。

然而，内部审计提供价值的方式不一定是通过网络安全相关的知识，可能会通过其在风险确认、风险交流领域的知识以及评估应对风险的控制措施来实现。这些也是 SEC 提案中想要针对某一特定风险进行强调的要素。

Watkin-Child 说："事实上，这些提案并非针对网络安全提出的，而是针对网络安全的风险管理提出的，意识到这一点十分重要。当人们想到网络安全，通常都会想到要采取控制措施，并开启恢复工作。这与 SEC 的期待完全不同。他们希望组织能够对网络安全风险进行评估。他们希望组织的董事会建立相应的治理结构，用于评估和确认对网络安全风险管理项目的监督工作，对其采取的具体形式并没有严格的要求。"

美国房屋抵押贷款供应商 Caliber Home Loans 的首席审计执行官 Manoj Satnaliwala 说："SEC 希望董事会承担起监督和确认职责。关键其实并不在于建立网络安全的标准，这些只是指导组织行动的框架，例如美国国家标准与技术研究院（NIST）的'网络安全框架'。"真正的难点在于落实责任，否则很容易变成相互推诿的一笔烂账。

内部审计的作用就是协助保持这其中的平衡。Satnaliwala 说："董事会和管理层需要协助。内部审计通过确认服务来确保自身的可信度，且通过提升组织内部各项事务的透明度来促进风险共担。风险的形式虽然各不相同，但内部审计的职责却始终如一。审计职能部门无需从头学起，组织也没理由要求每一个内部审计部门熟知网络安全项目的具体细节，而对于这项挑战来说，内部审计只需要拿着 SEC 的提案然后问'SEC 的期待是什么？'只要还掌握着一些网络安全资源，在我看来，一般的内部审计部门只需调整工作方法，确保按照提案要求将相应的风险纳入业务范畴即可。"

然而，掌握网络安全资源知易行难。通过培训和获取资格认证的方式来获取网络安全方面的专业知识不是一朝一夕能够完成的事情，尤其是规模小、预算资金有限内部审计职能部门，难以负担招聘高端人才的成本，除了在工作流程方面做到合规以外，在履行其他职能方面也十分受限。在这些情况下，内部审计必须全面了解获取知识的渠道，其中可能包括：

- **组织内部的人才储备。**在传统信息技术审计领域工作过的审计人员通常都具备一定的知识基础，能够相对快速地完成网络安全相关的技术培训。此外，一些网络安全的基本知识还可以并入变革管理、访问控制、信息技术运营以及灾后恢复等领域之中，从而降低长期外包服务的需求。

[10]. 国际内部审计师协会（IIA），《2022 年北美内部审计脉搏动态报告》

- **与组织治理第二条线和值得信赖的外部审计职能相互协作。**虽然根据《国际内部审计专业实务标准》的要求，我们必须要维护内部审计的独立性和客观性，但是与信息技术等相关职能部门建立更加密切的协作关系能够为审计人员间接获取技术能力提供便利，从而降低审计人员获取相关技术技能的难度和成本。

结语

亟需做好准备

随着负面因素不断发展和变化，企业们纷纷创新遏制负面因素的方法，网络安全问题也随之不断向前发展。2022 年将成为网络安全不断发展过程中里程碑式的一年，一项遏制网络安全问题、影响波及整个商业领域的措施应运而生。虽然 SEC 的提案还需要经过为期 60 天的意见征询期才能正式生效，但对于上市企业及其内部审计职能部门来说，已然是板上钉钉的事情了。

内部审计有能力也应该利用这段时间对组织内纳入网络安全战略需要的资产进行一次全面的统计和清点。否则内部审计人员将很难对组织现有的网络相关控制措施、政策和治理战略是否充分进行评定。这些评估工作不仅对组织的安保问题十分重要，对整个市场的安全也十分重要。全球各地之间的相互联系愈加紧密，这也意味着有关网络安全等领域的风险责任共享程度也逐渐提升。历史曾不止一次证明，一个组织受到攻击很可能会同时影响另一个组织的安全。

链条的坚固程度取决于其中最薄弱的一环。

第二部分

关键的伙伴——内部审计和首席信息安全官（CISO）

专家简介

Jerry Perullo

Jerry Perullo 是网络安全程序战略和治理公司 Adversarial Risk Management 的创始人，该公司致力于帮助企业快速建立成熟的网络安全程序。Perullo 具有 20 多年在纽交所等全球关键经济基础设施的网络安全项目中承担搭建和领导工作的经验，之后任洲际交易所（NYSE：ICE）首席信息安全官，并在退休后创立了 Adversarial。Perullo 拥有 NACD 董事资格认证®，还曾在金融服务信息分享和分析中心（FS-ISAC）担任理事六年，最近担任主席职位。Perullo 还担任乔治亚技术协会网络安全和保密专业实务教授，并开设讲座，通过他的网站 lifeafterCISO.com 分享自己的经验。

Hassan NK Khayal, CIA, CRMA, CFE

Hassan NK Khayal 是来自迪拜的一位内部审计经理。Hassan 被国际内部审计师协会评为全球 15 位 30 岁以下先锋领导者之一。Hassan 拥有 BBA、MBA 以及中东研究资格认证。Hassan 还拥有 CIA、CRMA 和 CFE 资格。他还拥有机器人流程自动化（RPA）、数据分析、物流网（IoT）、质量管理、健康和安全、环境管理和风险管理领域的专业资格。

Alan Maran

Alan 目前担任 Chewy 公司的首席审计执行官（CAE），他自 2019 年起进入这家公司，在担任 CAE 期间，他承担内部审计战略和执行工作的整体监督职责，包括对企业风险进行评估，为管理层的各项活动提供持续及时的咨询支持，为组织就应对关键风险的控制措施的适当性提供确认，协助维护组织运营、企业系统和信息技术相关的治理、风险和合规问题的一致性，持续关注内部审计团队成员个人发展，加强对数据分析、网络安全、数据保密的关注程度。Alan 是一位自身的审计高管，拥有超过 22 年在电子商务、金融科技、技术和制造业公司工作的经验，一直对学习保持积极的热情。在加入 Chewy 之前，他曾在安永会计师事务所担任进取型领导职务，之后又在多家跨国 500 强企业内部审计部门任职。他拥有 MBA 学位，以及华盛顿州立大学金融硕士学位，拥有注册舞弊审计师（CFE）资格，是一位注册区块链专家，是国际内部审计师协会地区分会会员。

Srini Srinivasan, PMP, CBIP

Srini Srinivasan 是 Chewy 公司首席信息安全和数据官。自 2019 年 10 月加入 Chewy 以来，他曾担任公司安全、数据和企业系统部门的领导，负责组织信息安全、数据和分析平台管理、企业系统和信息技术治理、风险和合规领域的监督工作。Srini 是一位经验丰富的技术执行官，拥有 25 年以上从事泛电子商务、银行和金融服务、零售和营销领域相关工作的经验。在加入 Chewy 之前，他曾在公民金融集团担任领导职务。他本人拥有巴拉迪大学计算机科学学士学位和本特利大学 MBA 硕士学位。

简介

建立伙伴关系对网络安全至关重要

网络安全一直是所有组织面临的重要风险之一。各项调查结果表明，网络犯罪分子一直在不遗余力地入侵敏感数据，诱导未经训练或毫无戒心的人泄露敏感信息或引入不良因素。

举例来说，2022 年《Verizon 数据泄露调查报告》显示，2021 年勒索软件相关的泄露案件增加 13%，高于过去五年上涨数量总和。然而，报告发现大多数成功的勒索软件采取的攻击方式是一致的——Verizon 报告数据显示，主要的攻击方式为入侵桌面共享和远程获取软件（40%）和电子邮件（35%）。[11]

国际内部审计师协会（IIA）最新指南《审计网络安全运营：预防和发现》（GTAG）旨在帮助组织检查对网络安全运营进行的确认工作，并提高组织对这项工作的重视程度。其目的在于帮助内部审计人员确定网络安全运营工作及其组成要素，将信息技术控制框架中的相关控制指南纳入考虑，并了解审计网络安全运营的工作方法。

指南中没有提到的完善网络安全确认工作的关键是建立和维护内部审计的领导与首席信息安全官（CISOs）之间的良好关系。这项潜在的互惠关系能够为管理扩展网络安全风险档案提供支持的同时，帮助内部审计与各类框架、风险和控制措施种的信息安全保持一致。

这项全球知识摘要阐述了内部审计领导与其负责信息安全事务的同事建立良好关系的有益之处，在确保内部审计独立性的前提下，寻求建立并维护此类关系的方法，并对此类关系如何为组织增加价值进行评估。

[11].《2022 年 Verizon 数据泄露调查报告的 3 个启示》，J. Mack， Rapid7，2022 年 5 月 31 日，https://www.rapid7.com/blog/post/2022/05/31/3-takeaways-from-the-2022-verizon-data-breach-investigations-report/.

全面应对网络安全问题

应对网络风险需要企业采取全面措施

网络安全一直是一个不断发展变化的风险领域，网络犯罪情况的复杂程度和总体数量逐年增长。大量数据表明，各个组织都极易受到网络攻击的影响。与此同时，各个行业的组织面临的压力也越来越大，不仅需要建立数据驱动的，高度依赖数据收集、管理、分析和使用的商业战略措施，还要利用新型技术改善组织绩效，提升整体水平。

正如组织对待其他重要风险领域一样，组织的各个领域都应该了解和管理网络风险。然而微软和 Marsh（保险代理商、风险管理公司）出具的报告《网络韧性现状》数据表明，很少有组织能够采取全面的措施管理网络安全。报告以一项针对 600 多位网络风险决策者的问卷调查[12]为基础，发现只有 40%的组织在制定网络风险规划中纳入了法律、公司计划、财务、运营或是供应链管理相关内容。[13]

报告称："信心不足的重要原因在于大多数的公司没有针对网络风险采取全面性的应对措施。增强自身网络风险应对能力，核心在于各个利益相关方在关键决策制定时要保持广泛的沟通，不断加强协作，提高一致性。"

报告确定了以下几项关键的风险趋势：

"由于每个组织都可能会受到网络攻击，网络相关的公司整体性目标—包括网络安全措施、保险、数据和分析，以及事件应对预案—应该与提高网络风险应对能力保持一致，而不仅仅是预防网络安全案件发生。"[14]

内部审计的领导者可以通过建立和维护与首席信息安全官（CISO）的关系，从而为企业采取有效的全面性工作方法提供巨大的支持。此项关系必须建立在双方拥有共同的目标，并且能够做到互相理解，彼此尊重的基础之上。

资深 CISO、Adversarial 风险管理公司创始人 Jerry Perullo（曾在纽约证券交易所母公司洲际证券交易所任职）认为，沟通不畅，或是缺乏对信息安全以及内部审计职能的了解可能会影响应对网络安全的一致性。相反，内部审计与信息安全部门的领导之间建立良好的关系有利于深化彼此对组织目标、战略、运营和政策的理解，从而帮助内部审计——通过扩大内部审计发现和建议的影响——增进与网络风险领导、高管层和董事会的关系。另外，内部审计与信息安全团队建立密切的关系有利于更好地宣传每个领域的关键使命以及双方支持组织提升全面网络安全水平的具体做法。

Perullo 说："最后，内部审计希望能获取更多有关信息安全方面的知识。虽然有很多种办法能够做到这一点，但是都比不上直接向信息安全团队学习更有效。"

Perullo 在为创业公司提供咨询服务时，通常开始就为组织设立网络安全治理程序，其中包含建立一个跨职能部门的网络安全治理委员会，将高管层、财务、法务和信息安全部门纳入其中。他表示，在这些程序中他还会指定内部审计高级管理人员作为观察员。

[12].《2022 年 Marsh 和微软网络风险调查》

[13].《网络风险应对能力现状》，Marsh 微软，2022 年， https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html?utm_source=forbes&utm_medium=referral-link&utm_campaign=gl-cyber-risk-2022-the-state-of-cyber-resilience.

[14]. 出处同上。

成功的五项关键要素

内部审计与 CISO 关系稳固的裨益

内部审计和 CISO 之间建立良好的伙伴关系有百利而无一害。双方之间关系的具体情况可能会因为组织的规模、各个行业的监管水平，或是组织的网络安全风险情况而有所不同。但是，无论组织规模大小，或是属于何种行业，双方的相互协作定能在以下五个领域产生明显的裨益。

深入了解并及时跟进组织的网络风险状况

风险状况是对组织面对的某种威胁的量化分析结果。从网络安全的角度来说，分析结果能够确定资产和网络风险，对用于管理这些风险的政策和措施进行检查，并尝试了解可能存在的漏洞。内部审计对网络风险状况的理解是后续制定审计计划的基础，审计计划不仅要支持组织采取应对网络安全的全面措施，同时还要提升内部审计在这一关键领域的相关性和价值。

线上宠物食品和宠物相关产品公司 Chewy 上市之后，公司内部审计领导 Alan Maran 利用三年时间与组织的 CISO Srini Srinivasan 建立了稳固的关系。Srinivasan 称信息安全要与内部审计、法务和其他利益相关方建立伙伴关系，基于 NIST 网络安全框架，对公司的网络风险状况进行全面的评估和衡量。

Srinivasan 说："这只是第一步。之后我们要设定一个网络安全与组织治理的三年路线图，基于之前的网络安全框架评估结果对其进行完善和加强。现在我们每年会做一次评估，看一看我们是否能够进一步把握机遇，同时对我们整体风险情况的衡量方式进行评估。"

采取从一开始就与内部审计合作的工作方法，Chewy 公司将内部审计的确认和咨询服务纳入战略规划之中，并将不断提高企业的整体网络安全定位作为战略发展的目标。

Maran 说："我们不能只说'我们需要对信息技术和安全进行审计'，我们也需要支持他们的工作。从内部审计的角度来说，作为合作伙伴，我们要坚定地支持 Srini 和他的团队，完成整套战略规划的制定工作。"

Srinivasan 还称双方相互协作的另一个好处在于提前将信息安全和独立的确认服务纳入新的项目之中。换句话说，信息安全、内部审计和治理控制不再是事后才会采取的措施。

Srinivasan 说："项目开始以后，两个团队都要参与其中，并且要与工程团队、产品团队、业务团队等部门合作，询问他们做了哪些安全方面的考虑？是否遵循了最佳的实务方法？"

Srinivasan 称建立适当的程序和控制措施有助于确定、尽量降低、甚至消除网络风险，他说："因此，一旦项目正式实施，我们双方的工作都会更加容易，因为我们彼此之间能够最大程度的相互谅解。同时也有利于我们对审计控制措施或是对检查或智力控制措施进行评估"

了解各项职能

Maran 和 Srinivasan 之所以能够建立稳固的伙伴关系，主要是因为 Chewy 是一家上市时间相对较短的公司，从一开始就为这段关系的建立提供了机遇。同时也为后续 Maran、Srinivasan 以及他们的团队之间进行开放、高频次的沟通奠定了基础。

Srinivasan 说："这是一种在关键利益相关方之间建立透明且互信关系的理想方式，我们不想错过这个机会。"

Srinivasan 表示这不代表各方之间永远不会存在分歧。但当冲突发生时，稳固的关系能够使双方沟通更加顺畅，并最终形成一个互利共赢的解决方案。

他说："对内部审计有所隐瞒对于我来说没有好处。他们对我们的工作越了解，就越能为我们提供更多的支持和帮助。从内部审计的角度来说同样如此，可以说我们彼此之间是不存在嫌隙的。"

最后，Srinivasan 表示，双方相互协作的工作方式能够提高运营的灵活度，内部审计的参与有利于发现和解决工作流程中存在的纰漏。

Maran 补充道，两个团队坦诚互助，从而进一步确定和巩固了对彼此之间职能的理解。

他说："Srini 并不会认为我们了解所有的情况，但同时他很尊重我们提出的观点和看法。"

确保相关性

无论在何种风险领域，在正确的时间提供确认意见，并发现关键问题都是内部审计面临的最大的挑战之一，在网络安全领域尤为如此。网络安全是一项不断变化，且发展迅速的风险，对确认服务的相关性和时效性要求很高。

Perullo 提醒到，内部审计的业务工作和相关建议如果与组织的网络安全使命相违背，对组织而言将是弊大于利。这些工作和建议在信息安全工作中造成一些模糊不清的情况，使外界不能确定内部审计想要看到的情况，尤其是在内部审计也不确定的情况下。

他说："内部审计可能在开始的时候并不确定自己想要看到的是什么，因此最好能够协作完成事前审计，对网络治理流程进行观察，从而确保审计工作与网络安全使命保持一致。"

Hassan Khayal 是一名拥有网络专业知识的内部审计顾问，他表示这是一个内部审计很容易受到指责的风险领域。内部审计人员常常以保护内部审计独立性为由，抗拒结识信息技术或信息安全团队的成员，以及了解更多相关的情况。

"当初我接手第一项业务时，我对信息技术的工作人员说：'我到这来就是向你们学习的。'我会预约一位了解工作程序，或是相关技术的工作人员共进午餐，向他了解他所在团队相关工作的具体细节。"

Khayal 表示这个学习的过程将帮助内部审计人员了解组织网络安全的成熟度，对日后提供相关的建议十分重要。

他说："对于小中型企业，或是尚未上市的大型企业来说，我们能做或是应该做的事情还有很多。在某种程度上，我们提出的建议可能会因为攻击性太强而无法实现。"

在内部审计与信息安全团队之间建立稳固的关系有利于降低审计业务和建议的不相关性或误导性。Chewy 公司已经证实了这项关系建立的好处。

Srinivasan 说："Alan 的团队和 Alan 本人通晓我们整体的安全战略，了解从技术的角度来看我们正在做什么以及我们面临的主要风险有哪些。因此在风险评级和我们的内部能力之间并不存在巨大的差距。这也将继续帮助 Chewy 团队、团队成员以及我们领导团队的整体知识水平。"

与董事会和高管层沟通

Chewy 的组织文化支持各职能部门之间进行开诚布公的沟通，有利于更好地了解组织的风险状况。Maran 和 Srinivasan 已经承担起报告的职责，向利益相关方——高管层和董事会——汇报双方团队相互协作的情况及其产生的积极效果。

Maran 说："目前很多组织都采取的是筒仓式工作方法，比如'如果是信息技术安全问题，就去找 CISO，他来负责这方面的工作。'但是从综合性风险管理或是企业风险管理的角度来说，我们发现的任何一种风险都有可能影响整个企业的发展。网络攻击可以会影响组织运营、产品交付以及财务工作。Srini 还成功向领导层报告了我们正在做的工作以及我们正在试图解决的风险情况。因此，从这个角度来说，两个团队之间实现了相互协作。"

团队之间相互协作也有利于及时且灵活地应对不断变化的风险和网络监管环境。例如，Maran 和 Srinivasan 表示团队有信心协助组织应对美国证券交易委员会 2022 年第一季度发布的有关网络安全报告的最新规定。

团队之间的相互协作也不仅局限于信息安全和内部审计领域。Srinivasan 说：“除了要关心组织的安全问题以外，我们还有其他关键的利益相关方，因此我们也与会计和法务团队建立了类似的伙伴关系。在我看来，团队之间坦诚互信的伙伴关系能够支持我们更好地应对不断发展的监管规定和其他要求。”

Khayal 提醒道，尽管连续且统一的信息传递让 Chewy 公司的领导团队受益良多，但当领导团队不能及时了解组织的网络状况和需求时，将会给组织带来巨大的危险。他表示，如果领导层对信息技术和网络安全缺乏了解，那将造成巨大的财务损失。Khayal 表示，如果内部审计不愿意了解组织信息安全状况，则很难在这一领域提供有价值且有相关性的确认服务。这也将影响管理层和董事会对网络安全的认识。

保护和尊重独立性

Khayal 正在努力取得注册信息系统审计师（CISA）资格认证，为了获取这项资格，他开始不断努力提升自己在信息技术和信息安全方面的专业技能。而且他也不断增进与同级别的信息技术部门的同事之间的交流互动，他们也越来越愿意为其主动提供对于审计人员来说更加先进或复杂的信息。此外，他认为这种互动并不会影响他在开展审计业务时确保审计工作独立性和客观性的能力。

他说：“我们每天大多数的时间都是在办公室度过的。审计人员确实应该保持独立性，但我个人认为这并不代表审计人员不能在工作中结交朋友，每天只能自己一个人吃午餐。”

Khayal 称他利用这种方法处理和组织所有部门之间的关系。他会和计算机领域的同事讨论 Linux 系统，或是与市场营销部门的同事讨论社交媒体相关话题。

他说：“这是一个很好的机会，既能培养专业技能，又能维护与其他同事之间的关系。这就像是我们对审计客户或被审计单位说‘我们正在对工作流程和交易进行审查，但我们并不是针对某个人。’因此，当我们和他们一起吃午餐时，也与工作流程和交易的审查工作没有关系。”

Maran 表示，在 Chewy 公司，Maran 和 Srinivasan 之间密切的工作关系给彼此之间独立的确认工作提供了相互的理解和支持。

他说：“内部审计职业的本质是在核查的基础上的信任。从客观性的角度来说，我有责任这样做。因此，的确我们彼此之间相互信任，尤其是在对出现变更的情况进行检查的情况中。绝大多数情况下，我们证实事情并没有发生改变。但是我还会对管理层提供信息的完整度和可信度进行检查。我们不会只看报告的表面价值，我们会追踪溯源，从而确保最终结果的完整性和准确性。”

Maran 称，总而言之，充分了解组织各方的职能能够使工作变得更加简单。

他说：“我们之间存在一个共识，那就是内部审计究竟要做哪些事情。我们需要提供为高级领导层——董事会、利益相关方以及审计委员会——提供确认服务。我们就本年度的审计工作和审计范畴达成一致意见。虽然有的时候我们也会讨论各自的观点和看法，但是我们对需要提供确认服务的风险领域的认识是保持一致的。”

Srinivasan 补充说到，我们才能在网络安全问题上采用数据驱动工作方法的前提是信息安全部门和内部审计就事实情况达成一致。

他说：“如果意见存在分歧，我们需要努力统一对事实的掌握情况，然后我们就能够站在相对客观的角度说‘这个问题比较关键、十分关键或是不太关键’。我想这样一来我们就能顺利推进问题的讨论，并达成相应的结果，而不是毫无头绪的争吵不休。”

增加价值

增强网络安全的韧性

Srinivasan 称他从始至终都坚守 Chewy 公司的使命，具体包括三个方面的内容：遵循公司内部运营的原则，保证信息安全和内部审计的一致性，以及通过提高透明度建立彼此之间的信任。

他说："我们已经坚持了很长的时间，而且从团队成员和领导层的角度来看，努力已经看到了回报，我们做到了及时跟进最新的发展情况。"

如前所述，增进沟通、互助和合作有利于提高工作的灵活度，使内部审计逐渐参与到网络安全流程之中。Srinivasan 称主要的因素，如对可持续性重视程度不断提高、供应链的相关考虑、市场状况、地缘政治发展等都要求组织采取更加有效的方法，应对网络安全问题，并进行相关的确认。

他说："这些情况都迫使我们提高自身的敏锐度，及时有效地应对出现的问题。如果我们还是遵循传统的、按部就班的的工作模式，不设法缩短工作周期，就一定会错失良机。因此，我对目前公司的业务安排十分满意。"

扩展知识储备

建立伙伴关系的另一个好处就是，两个团队能够提高对彼此工作的理解和认可度，从而有助于实现共同的目标——确保组织网络安全。

Maran 说："我们经常会就彼此的技术知识进行讨论，如'我们检查过这方面的问题吗？你考虑过那项问题吗？这是我对这项风险分析的看法，跟你的观点是否一致呢？'因此，从一开始我们就已经在考虑要关注哪些问题，而且 Srini 也会参加进点会。我们开始审计之前他就会参与讨论。因此不会出现意料之外的情况。"

但是只有审计业务正式开始实施，内部审计与信息技术和安全人员直接接触时，才会产生真正的价值。

Maran 说："从职业发展的角度来看，尤其是站在信息技术和网络安全的角度，与传统的勾选框式审计方法相比，这种工作方法确实更有效果，能够掌握更多的信息，例如对具体情况的阐述，以及问题恢复需要的技术知识等。在我看来，我们的团队从中获益良多。"

结语

内部审计与信息安全部门之间建立良好的关系能够给组织带来很多益处，主要体现在能够促进组织对网络风险认识的统一性，其中包括组织的薄弱环节、发展机遇、成熟度以及穿透测试等。

此外，一旦组织出现网络事件，影响网络安全的因素发生变化，或是监管环境发生变化时，稳固的关系有利于提高组织应对风险的韧性和灵活度，有助于为高级管理层和董事会提供统一的有关网络安全风险、需求、工作重点和健康发展的信息。当两个团队能够深入理解和认可各自的职能、工作方法和责任，内部审计的独立性将会得到保护，甚至是加强。最后，审计部门领导和 CISO 之间稳固的关系能够支持企业采取全面的网络安全措施，从而加强信息技术安全水平。

Maran 说："我们的观念正在从单纯的审计——'我的工作就是开展评估工作，并提出有意义的观点和看法。'转变为'这是我的公司，这是我真正关心的问题，要通过我们的努力来帮助团队取得成功。'"

第三部分

网络事件的应对和恢复

专家简介

Brian Tremblay

Brian Tremblay 是 Onapsis 公司合规事务部的领导，负责帮助客户了解和驾驭当前信息技术综合控制、监管和合规，如萨班斯·奥克斯利法案（SOX）和通用数据保护条例（GDPR），领域不断增叠的合规、网络安全和商业持续性带来的机遇和挑战。在加入 Onapsis 之前，他曾在高科技半导体公司 Acasia Communications 担任 CAE。除了建立并领导组织所有的内部审计活动以外，他还曾协助组织上市相关工作（包括 SOX 实施工作），并协助组织实施全面风险管理（ERM）政策。再之前，Tremblay 曾在美国铁山公司（Iron Mountain）担任内部审计总监，负责北美地区所有审计和项目工作，同时还负责与全球质量经理的联络工作。在加入铁山之前，他曾担任霍顿米夫林出版公司高级经理，帮助公司建立了内部审计部门，并开始实施 SOX。在职业生涯的初期，他还曾在雷神公司和德勤会计师事务所任职。

DaMon Ross Sr.

DaMon Ross Sr.于 2020 年创立了网络防御国际集团，他和他的团队凭借优异的网络安全运营和网络威胁智能应对技术，为缺乏相关经验和技术的组织提供适当的网络安全解决方案和服务。在创立网络防御国际集团之前，Ross 曾在 SunTrust 银行担任网络安全运营高级副总裁，创立了 SunTrust 全天候网络安全运营中心。Ross 组建了负责网络智能、网络威胁监控、网络事件应对和网络犯罪问题的专业团队。他还成功与法务、人力资源、企业安全、企业道德和风险部门的同事建立了伙伴关系，共同搭建了银行首个内部威胁监控项目。Ross 还协助公司与美国特勤局电子犯罪特遣队和美国国土安全部等多个组织建立了信息共享的伙伴关系。

简介

回归基本要素

长期以来，网络安全一直是各个组织及其内部审计职能部门关注的重点问题，2022 年也绝非例外，美国证券交易委员会（SEC）今年出台了有关网络安全风险管理、战略、治理和事件披露的新提案。这些提案和其他监管规定的出台绝非偶然。身份盗窃资源中心的报告显示，2021 年共有 2862 起登记在册的数据泄露案件，较 2020 年上涨 68%，这一数字也超过了此前 2017 年创下的有史以来最高纪录。所有行业都受到了这一严峻形势的影响。[15]

在这种环境下，组织希望，也的确需要建立清晰、有力的网络安全控制措施和程序，其核心基础是组织要持续跟进了解风险及相关监管规定，并保持董事会、管理层以及内部审计部门之间的沟通和一致。IIA2022 年网络安全报告的三个部分内容中，第一部分重点阐述了可能存在的监管影响，第二部分讲述了首席信息安全官和内部审计团队建立稳固关系的各项益处。最后第三部分讲对组织网络事件应对策略的制定和实施进行重点描述，具体来说，为尽快从网络安全泄漏事件中恢复过来，组织制定了关键的控制措施。当内部审计对这些控制措施进行评估时，如何才能为组织提供价值。

[15]. 身份盗窃资源中心，《身份盗窃资源中心 2021 年年度数据泄露报告 数据泄露创下新高》，2022 年 1 月 24 日，https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

关键的控制措施

让内部审计参与到网络事件应对之中

有关网络事件应对的错误认知

虽然“网络事件应对”和“网络安全应对和恢复”都是准确且有益的定义术语，但从某种角度来说，并没有完全概括出有效的行动规划所有的要求。

内部审计最核心的职能是为组织提供有关风险管理的独立确认服务。不仅要对组织在网络事件应对方面是否妥当提供确认，还要对控制措施进行适当的评价，以确保组织能够减轻风险的程度以及风险对组织的影响，或是在理想状态下，防止风险的产生。为了实现这一目标，内部审计不能把关注点只放在风险应对方面。相反，内部审计应该从整体性、周期性的角度看待网络事件的应对，将工作重点放在预防性控制措施和积极应对措施方面，从而改善应对工作的成效。

Onapsis 公司合规部门领导 Brian Tremblay 说：“风险管理就如同车轮一般，开始的时候我们要采取正确的控制措施，并按照我们认为正确的流程推进工作进展。之后，当问题出现时，我们之间的对话将立刻变为‘控制措施的效果是否符合预期，我们之前预测会发生的情况是否真的发生了？’此后，我们要吸取教训，做出改变，并重新回到开始的地方。组织的现状和未来的发展对我们来说同等重要，因为我们不仅要处理当下的问题，还要为未来的发展考虑。鉴于组织常常为此类问题困扰，内部审计也应该越来越重视这个领域的工作。”

不会改变的基本要素

通常情况下风险状况会越来越复杂，而且由于网络安全本身技术性程度很高，随着科技的进一步发展，我们在了解风险本身以及减轻风险所需的系统方面遇到的阻碍会越来越大。然而，这并不完全代表网络事件应对计划和控制措施的基本要素会发生巨大的变化。

IIA 在最新的补充指南：《审计网络事件的应对和恢复》中列举的控制措施大体可以归纳到以下四个高层次的业务目标之中：

- **事件应对规划。**组织应该制定相应的政策和流程，为确定网络事件是否发生以及如何应对提供指导。规划中应该涉及关键的利益相关方、定义角色和职能，同时要测试其是否能够提升组织风险意识和执行能力。
- **事件判定。**通过对控制措施中的数据进行分析可以判定是否有网络事件发生，通常情况下这触发后续一项或多项应对预案的实施。
- **沟通。**在网络事件中有很多潜在的利益相关方，因此每项应对预案都应该包括一项沟通策略，从而确保能够及时有效地向利益相关方报告事件的影响和解决办法。
- **技术方面的应对措施和恢复情况。**网络事件的本质很大程度上决定了采取哪些必要的技术补救和恢复控制措施，通常情况下会涉及内外部职能的相互协作。[16]

[16]. 国际内部审计师协会，《审计网络事件的应对和恢复》，补充指南，实务指南，https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/2022/gtag_auditing_cyber_incident_response_and_recovery_final.pdf.

为了完成这些业务目标，同时遵守美国国家标准与技术研究院（NIST）《提升关键基础设施网络安全框架》等网络事件应对框架，需要掌握有关技术实施、维护和完善的相关知识，这些知识通常是由信息安全和信息技术团队提供的。虽然内部审计不一定会掌握这些知识，但是同样能够为组织提供同等的价值。内部审计凭借其在组织内的特殊地位，能够获取并了解组织各职能部门的情况，并在为组织提供客观确认方面提出独立的观点和立场，从而为组织提供相应的价值。

网络防御国际集团创始人、SunTrust 前高级副总裁、网络运营主管 DaMon Ross 先生说："从内部审计的角度来看，网络事件的应对方法与其他风险并无二致，其核心都在于实际采取的工作流程及其产生的效果。即便网络事件的技术含量很高，熟悉风险应对流程的审计人员也能快速找到问题的关键之处。"

这种流程与《萨班斯·奥克斯利法案》（SOX）的合规程序、危机应对预案或是任何一种风险管理战略都十分类似。Ross 说："不同的组织使用的术语各有不同，但是网络事件应对预案的核心是一项组织治理政策，阐述网络事件发生的时间、所有相关方的角色和职责以及由谁来负责做出决策。"

Tremblay 也表达了类似的观点。他表示，与网络风险相关的控制措施依然是属于 SOX 中管理合规风险的框架内容。

例如，黑客攻击任何一种技术时，第一步都是要获取必要的授权，从而达成自己目标。从宏观角度来看，这属于未经授权访问风险。Tremblay 认为无论是从 SOX 还是从网络风险的角度来说，这一点都是一致的。他说："当我们追溯风险最原始的形式时，用于消除风险的控制措施从根本上来说都是一致的。"

文件编制控制措施

正如 Tremblay 所述，网络事件相关政策包含的控制措施与其他组织面临的风险相关的控制措施有很多重合之处，有效的文件编制流程就是其中之一。Ross 也同意这一观点，他表示组织必须了解网络事件相关文件的编写流程，以及如何确保所有同步开展的活动能够并行不悖。

Ross 说："这一点不仅适用于大的网络事件。每个组织都应该配备一个单独的职能，用于处理日常发生的网络事件。例如电脑出现病毒，这类问题虽然很小，但很可能会发展成为大的网络事件，当问题进一步恶化时，适当的文件记录有助于职能部门了解问题恶化的原因，从而采取相应的控制措施。"

问题检测以及基础设施控制措施

基础设施是另一项关键的控制措施，也是用于衡量未经授权获取风险的工具。虽然当我们讨论网络安全问题时，可能不会立刻想到这类控制措施，但是 IBM Security 发布的一项源于 Ponemon 机构的调查数据显示，在 2020 年所有的恶意网络攻击事件中，未经授权入侵存有敏感信息的硬盘或服务器的事件占比为 10%，平均每次数据泄露给组织带来的损失高达 436 万美金。

因此组织需要配备相应的基础设施，如限制安全服务器房间准入，同时还可以设置一些更加基础的安保措施，如安装防盗锁装置。虽然基础设施安保十分重要，组织依然要配备适当的控制措施，用于发现和记录可能存在的可疑活动。

Tremblay 说："我所说的基础设施，指的不是把门锁起来，而是要对可能造成风险的情况进行通报和记录。这才是问题的重点，是一顿饭的主菜，而不仅仅是开胃菜。"

Ross 表示，为这些系统问题提供确认服务正好属于内部审计的职能范畴，他补充说到："内部审计有能力发现可能为组织存续带来重大风险的系统。事实上，内部审计在为其他风险的合规问题提供确认服务时，已经找到了存在风险的系统。我们需要做的是进一步拓展这样的思考方式，利用新形式的配置来延申至更高层面。

统一对事件恢复的期待

对网络事件应对预案所有层面的情况进行有效记录是十分关键的。但是，同样关键的是对记录文件中的数据进行沟通交流，并统一组织在发现问题和事件恢复方面的期待。

Tremblay表示在他看来这是组织在网络事件应对预案方面存在的最大问题，也是内部审计能够提供最大价值的领域。他说："内部审计在网络灾难恢复中扮演着双重角色，一方面，要确定网络事件是否存在，内部审计可以通过记录文件或使用任意技术或工作流程来证明网络事件的存在。另一方面，也是我认为内部审计欠缺的一方面，要与所有关键的利益相关方坐下来，基于组织的风险偏好，确定网络事件恢复的时间表。

Tremblay 称网络事件恢复时间表将由组织内相关的应用"责任方"建立，其中有可能是 CISO、供应链领导或是其他领导，取决于网络事件具体发生的领域。内部审计的关键任务是承担这个"责任方"和在日常工作中依赖此项应用的其他部门之间的纽带。

Tremblay 说："例如，CISO 可能认为只要在 48 小时之内完成恢复就可以，但是如果我们没有询问 CFO 或者其他依赖此项技术开展工作的职能部门的意见，那么我们后续可能会遇到很多麻烦。例如，CFO 表示可以接受 48 小时之内恢复，但前提是不能发生在财务决算期间。因为在决算期间，财务电脑不能停机，否则组织需要申请延期，这在公开市场上造成十分严重的负面影响。"

但与各个职能部门沟通并不意味着只关注某些部门而忽略其他部门的需求。相反，通过增进沟通，内部审计能够根据组织的风险偏好来协调各方需求，并达成共识。Tremblay 说："当各方存在差异时，内部审计可以提问'这样做真的值得吗？'CEO 可能会说'是的，因为解决这项问题需要花费一百万美金。'我们真正要做的是确保能够根据利益相关方的需求以及技术的特点制定相应的应对预案。"

他继续说到："在我看来，这并不是我们内部审计职业十分擅长的领域。内部审计人员利用勾选框式的审计方法，对具体事项进行确认，而不是真的说'在对事件应对控制措施进行检查时，我们发现组织在某项技术方面没有达到利益相关方的要求。'这是合理的。意味着我们发现了一项对组织来说很有价值的，之前未被发现的业务风险。"

跨职能性

我们普遍认为应对网络安全问题主要是由 CISO 和安保团队负责的，这其实是一个误区，其中只有部分内容是正确的。虽然这些职能大概率掌握着网络战略中很多技术工作所需的工作经验和专业知识，但是我们绝对不能认为他们有能力或是有意愿独立承担这项任务。

Ross 说："网络事件应对至少应该是一项跨职能工作流程。在我看来，组织在应对网络事件中存在延时现象的最大原因并不是由于信息安全部门缺乏相关知识，而在于与其他部门建立跨职能协作的岗位和职责，安保问题不是这些部门的主要职责，他们还承担着其他的工作。"

Ross 表示，纠正这种错误的认知，鼓励所有利益相关方责任共担是内部审计需要关注的重点问题。他说："问题的重点不一定在于安保团队以及他们的工作，相反可能在于组织内其他相关部门是否对他们的工作给予了应有的支持。安保团队懂得如何解决问题，但是他们不能逼迫信息技术团队或是终端开发团队在关键之处给予协助。这项工作牵扯了很多的组织政治问题，当我身处其中时，我发现内部审计是一个很有价值的伙伴。安保团队不能单打独斗。你们需要找到一个中间方，协助确认组织在工作流程中存在的问题，这对每个人都有好处。"

Ross 认为为了能够强调存在的差距，明确各方的职责，可以依靠内部审计职能部门，他们通常与外部顾问团队相互协作，推进桌面模拟。他说："一旦我们将网络事件应对预案放在可测试的领域，桌面模拟就能把首席信息官（CIO）、CISO、信息技术部门领导、CEO、内部审计等所有利益相关方聚集到一起，通过线上或线下会议共同讨论演示可能会出现的情况。即便没有技术方面的专业知识，内部审计也能通过询问各方具体工作，并对这些内容与现实情况是否相符进行评估，从而协助推进会议进程。他们可能会说'在这个方面，根据我们的计划，你们应该做 X 和 Y，但事实上你们可能在做 Z。'这样我们才能了解事情的真相。大多数组织可能每年至少会组织一次这样的活动，但内部审计的确应该在其中起主导作用。"

结语

根据风险环境不断发展

内部审计凭借其在组织内的独特地位，应该在组织讨论制定网络事件应对预案中占据一席之地。同时内部审计也需要努力加深对网络安全的探索和了解。的确，未来物理基础设施将会快速被淘汰，转而依赖云计算为基础的新兴技术，因此，内部审计也必须根据需要掌握更多的专业知识。

Tremblay 说："当我刚开始从事内部审计职业时，内部审计最大的卖点在于这是一个多面手的角色。内部审计人员需要观察和学习很多领域的各种知识，我们对这些知识并不熟悉。但是近年来技术领域发生了巨大的变革，我开始思考，内部审计人员作为多面手的日子是不是已然屈指可数了。或者说，内部审计可能有一天会成为组织固有关键领域的主题专家。因此，与其在审计团队中配备 8 到 10 位运营、合规和财务报表审计员，组织应该配备一位网络安全审计员、一位环境、社会与组织治理（ESG）审计员…"

Ross 对此也表示同意，他说："随着新兴技术的不断发展，如果我们不深入了解具体情况，又怎么能知道应对程序真正存在的问题呢？可能永远都不能真正了解。"

掌握知识和资源有助于实现更多目标，我们即将迎来一个令人激动的新时代，内部审计也必须参与其中。

往期报告

访问 www.theiia.org/GPI 获取往期《全球观点与视角》。

读者反馈

请将您的问题或建议发送至 globalperspectives@theiia.org

关于国际内部审计师协会（IIA）

国际内部审计师协会（IIA）是一家国际职业组织，拥有超过 215,000 位全球会员和 180,000 位 CIA 持证者。IIA 成立于 1941 年，是在内部审计行业得到最广泛认可的国际组织，是内部审计的倡导者，为全球内部审计人员提供内部审计标准、资格证书、教育服务、调查研究和技术指导。更多信息，请浏览 theiia.org。

免责声明

版权说明

2022 年 8 月

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101