针对有效数据安全的必要假设

数据安全功能和依赖该功能的组织面临的最严峻挑战并不是技术问题，甚至不是迫在眉睫的网络攻击威胁。主要的挑战在于确保组织中的每个人达成一致意见，并根据同一组假设来制定决策和采取行动。

根据企业管理协会 (EMA) 的研究，许多组织都制定有区域或部门层面的安全运营计划，但这可能会导致资源浪费和事故响应时间增加等问题。[1] 特别是在数据安全功能预计将在后台运行以保障安全的组织中，数据安全与业务管理、技术和其他领域的关系可能存在不同的优先级、期望和假设。

为了确保数据安全工作有效发挥作用，企业各个领域和级别的人员必须根据与数据安全相关的五个关键假设开展工作。内部审计部门应在此过程中发挥关键作用。凭借其跨部门的影响力以及对组织范围内风险管理工作的了解，内部审计部门在促进必要的调整和评估是否发生问题方面具有得天独厚的优势。

1. 数据安全团队应采取综合方法

数据安全的每个重要方面几乎都在通过某种方式扩大范围。近年来，工作场所的定义、员工所在的地点、支持数据的各种业务流程以及最终用户设备的数量都在不断扩大。所有迹象都表明需要对信息和数据安全采取更广泛、更高层级、更综合的方法，而不是仅仅将其视为一个专门的独立问题。

因此，许多企业领导者坚持认为，他们在数据安全领域面临的最严峻挑战并不在于制定战术，而是纵观全局。在 2021 年的一项研究调查中，受访者被问到：“贵组织面临的最严峻的数据安全问题/挑战是什么？”排名前两位的回答是：

1. 整个组织的统一安全战略 (22.1%)
2. 数据复杂性/数据部署的复杂性 (16.2%) [2]

必须设立一支具有明确职责和责任的专门数据安全团队，但如果高级管理层和董事会秉持严肃认真的态度制定统一的数据安全战略，那么必须要求（并允许）数据安全团队在组织的各个领域采用更具交互性和更综合的方法。这包括与战略计划、产品开发和客户服务团队进行上游互动，以确保他们事前就考虑好数据保护问题，而不是事后才考虑。

KEVIN M. ALVERO | 注册信息系统审计师 (CISA)、数据隐私解决方案认证工程师 (CDPSE)、注册舞弊检查师 (CFE)

尼尔森公司内部审计、合规与治理部门高级副总裁。他负责领导内部质量审计程序及行业合规性计划，涵盖企业的全球媒体产品和服务。

BRIAN ALVERO | 注册敏捷领导力 (CAL)、注册敏捷教练 (CSM)、注册安全师 (CSP)、注册敏捷产品负责人 (CSPO)、注册六西格玛黑带 (CSSBB)

美国佛罗里达州帕斯科县警长办公室首席信息官和首席安全官。他负责领导整个机构的整体技术解决方案、举措和战略。

这种方法不仅有助于最大限度地减少数据安全漏洞，还有助于最大限度地提高效率。如果组织缺乏统一的战略，就更有可能将资金浪费在冗余工具或在组织的多个领域中不兼容的工具上。正如最新的 *Microsoft 数字防御报告*中所述：

> *组织必须能够审视其应用程序、端点、网络和用户……[他们] 还将通过采用更多内置于云端和生产力平台的安全功能来降低成本。为了最大限度地提高安全组织的效率，必须完全集成工具，从而提高有效性并提供端到端的可见性。*[3]

内部审计部门的作用

内部审计具有得天独厚的优势，他们可以审视整个组织，并确定不同业务领域之间的不一致和冗余情况。尽管谨慎的数据安全审计可能是有用的做法，但内部审计部门能更好地在其执行的每次审计工作中整合数据安全功能，以便随着时间的推移建立一致感。

2. 数据隐私计划可以创造竞争差异化

在许多组织中，数据安全团队的角色类似于体育运动官员；如果人们察觉不到他们的存在，就证明他们的工作确实很到位，而一旦大家注意到了他们，则往往是因为出现了严重问题。然而，数据安全职能部门和相关执行人员正在越来越多地走进大众视野。*CSO* 报告称，近一半的受访组织在 2022 年增加了网络安全支出，几乎所有组织都至少保持了这类支出与往年持平。[4] 与此同时，越来越多的组织决定，如果他们要在数据安全和监管合规方面花费大量资金，那么至少应该能够借此机会主动向客户讲述令人信服的故事。在上述调查中，超过 70% 的受访者表示他们可以使用或者已经使用其监管合规或数据隐私计划作为市场竞争优势。[5]

在欧盟《通用数据保护条例》(GDPR) 和美国《加州消费者隐私法案》(CCPA) 的带领下，未来几年数据隐私监管的规定可能会大幅增加，组织必须关注消费者的怀疑态度以及更加声势浩大的监管环境带来的机遇。那些仅仅将隐私法规视为约束的组织将逐渐陷入严重困境。为了抓住机遇，组织必须更好地与其客户就数据安全和信任-价值关系进行集体层面和个人层面的沟通，从而鼓励客户自愿交换信息以获取价值，因为第三方跟踪数据将越来越难获得。

为了抓住机遇，组织必须更好地与其客户就数据安全和信任-价值关系进行集体层面和个人层面的沟通。

麦肯锡公司最近的一份报告指出，“许多企业的数据隐私举措的问题在于，对于日常客户而言，它们过于技术化或过于法律化。”报告称，要想建立成功的数据关系，企业应考虑聘请一名全职数据关系经理。[6]

通过聘请沟通能力强且具备技术专业知识的人员，组织将能够以注重价值的方式引导其客户理解数据保护政策和技术，而不是让客户费力阅读使用条款并敷衍地点击“接受”。

麦肯锡报告进一步指出，

> *投资于这些数据关系管理要素的公司将有机会在数据保护方面占据领先地位，从而在未来几年坐享红利。*[7]

组织还需要更好地与自己的员工进行工作方面的沟通。常见做法是提供安全意识培训计划，但一些员工仍然对此有所误解，认为数据安全政策和相关人员主要是阻止他们做自己需要做的事情（让变通方案变成必须之选）或是让他们去做本不属于其责任范围的事情。与对待客户一样，主动向员工传递的围绕合规性的信息应该以价值为驱动，并专注于数据安全团队如何帮助组织及其员工取得成功，而不仅仅是控制风险。

内部审计部门的作用

从树立形象的角度来看，内部审计部门也处于同样的情况，他们可以帮助评估沟通工作是否易于理解且以价值为基础，以及是否呈现出数据安全使命的正面形象。

3. 零信任是大势所趋

传统信任虽然会验证网络安全方法，但它会自动信任组织边界内的用户和端点，从而使组织面临内部恶意行为者的风险，并且合法凭证容易被恶意行为者接管。[8] 随着员工越来越分散以及网络攻击愈演愈烈，对用户进行身份验证的零信任方法应该是每个组织依据或努力建立的范式。

根据 *Microsoft 数字防御报告*，多因素身份验证 (MFA) 是零信任框架的关键组成部分，可防止 99% 因凭据被盗而遭受未经授权的访问的情况。报告指出，“这意味着现在我们每个人都踏上了零信任旅程 — 无论我们是否察觉。”[9]

内部审计部门的作用

在了解组织控制措施的有效性和识别零信任环境中的潜在漏洞方面，内部审计部门是数据安全的关键合作伙伴。

4. 事故响应与事故规避具有同等的重要性

在国际灾难恢复协会的*第七次年度全球风险和恢复能力趋势报告* (Seventh Annual Global Risk and Resilience Trends Report) 中，[10] 根据调查受访者的回答，对组织的业务影响方面总体排名最高的三大威胁分别是网络攻击、IT 中断和数据盗窃。受访者是从包括疫情、自然灾害、供应链中断和气候变化等在内的 20 个潜在威胁列表中进行选择。

在事故响应方面，必须像对待事故规避一样尽职尽责且具有紧迫感。

与此同时，全球每周的网络攻击数量不断增加，2021 年第四季度 (Q4)，平均每个组织遭受了 925 次网络攻击，这一数字创下历史新高。[11] 安全专家普遍认为，每个组织都会成为网络攻击的目标，只是时间早晚的问题。

如果风险确实有可能发生并会产生影响，那么显而易见，每个组织的当务之急就是建立网络安全恢复能力。在事故响应方面，必须像对待事故规避一样尽职尽责且具有紧迫感。事故响应不仅应包括记录在案的计划，还应包括定期演练和强化行为，以便在检测到漏洞或攻击未遂后的关键时刻迅速采取适当行动。

内部审计部门的作用

内部审计部门可以发挥的作用包括提高对攻击频率和漏洞趋势的认识，以及将网络安全事故响应计划纳入到内部审计计划。此外，内部审计部门可以帮助将网络安全风险与业务影响联系起来，从而令业务领导者信服。

5. 数据不一定越多越好

由于启用大数据功能的应用程序具有无限可能性这一点充满了诱惑力，因此各个组织都逐渐接受了将数据视为关键战略资产这一理念，这样做也无可厚非。与此同时，考虑到数据泄露可能带来的法律、财务和声誉方面的损失，数据安全专业人员以及他们所服务的企业也必须留意与组织数据相关的潜在责任 — 而且风险呈现出上升趋势。据*《合规周刊》(Compliance Week)* 报告，2021 年对违反 GDPR 的组织处以的罚款金额近 12 亿美元。[12]

与此同时，2022 年 1 月，欧洲数据保护监督机构 (EDPS) 通知欧盟执法机构 Europol，要求他们删除与犯罪活动没有明确关联的个人数据。这是一个广为人知的例子，该组织因拥有监管机构认为不应拥有的数据而被公开点名批评。[13]

简而言之，并不是拥有的数据越多越好，而是应考虑到数据泄露的风险，根据数据的价值做出保留或删除数据的决定。

内部审计部门的作用

内部审计部门可以确保实施可靠的数据保留政策，并通过定性和定量审计技术来验证员工是否理解并遵守这些政策。为了证明审计工作的重要性，内部审计部门还必须传达未能做出明智的数据保留决策会带来的业务风险。

结论

如果组织的员工不了解广泛的数据安全战略以及他们在实现战略方面发挥的作用，并且也未就此达成一致，那么即使是针对当今网络安全问题的最精妙的技术解决方案，也可能会毫无用武之地。如果整个组织存在不同的假设和期望，甚至会破坏技术娴熟、资金充足的数据安全力量。因此，高层管理人员应明智地开展沟通工作，确保整个组织普遍了解关键假设。内部审计部门可以帮助建立统一的观点。

尾注

1 Steffen, C. M.；*Data Security in a Multi-Cloud World*，企业管理协会 (EMA)，美国，2021 年 8 月 11 日，*https://www.ibm.com/downloads/cas/6EODENGR*

2 *同上*。

3 Microsoft，*Microsoft 数字防御报告*，美国，2021 年 10 月，*https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi*

4 Pratt，M. K.；“Cybersecurity Spending Trends for 2022: Investing in the Future”，*CSO*，2021 年 12 月 20 日，*https://www.csoonline.com/article/3645091/cybersecurity-spending-trends-for-2022-investing-in-the-future.html*

5 *Op cit* Steffen

6 Brodherson, M.；A. Broitman；J. Cherok；K. Robinson；“A Customer-Centric Approach to Marketing in a Privacy-First World”，麦肯锡公司，2021 年 5 月 20 日，*https://www.mckinsey.com/business-functions/growth-marketing-and-sales/our-insights/a-customer-centric-approach-to-marketing-in-a-privacy-first-world*

7 *同上*。

8 Raina, K.；“Principles of the Zero Trust Model”，Crowdstrike，2021 年 5 月 6 日，*https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/*

9 *Op cit* Microsoft

10 国际灾难恢复协会未来愿景委员会，*Seventh Annual Global Risk and Resilience Trends Report*，美国，2021 年，*https://drii.org/crm/presentationlibrary?plsharekey=346cbc8d7c96e8c*

11 Muncaster, P.；“Corporate Cyber-Attacks Spike 50% in 2021”，*Infosecurity Magazine*，2022 年 1 月 11 日，*https://www.infosecurity-magazine.com/news/corporate-cyberattacks-spike-50/*

12 Hodge, N.；“Report: GDPR Fines Surpass $1B in 2021；Breach Notifications Also Rise”，*Compliance Week*，2022 年 1 月 18 日，*https://www.complianceweek.com/regulatory-enforcement/report-gdpr-fines-surpass-1b-in-2021-breach-notifications-also-rise/31259.article*

13 欧洲数据保护监督员，“EDPS Orders Europol to Erase Data Concerning Individuals With No Established Link to a Criminal Activity”，2022 年 1 月 10 日，*https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en*