电子档案信息安全风险评估与防范策略

冉忠慧

高阳县妇幼保健院

摘　要：在信息技术飞速发展的今天，电子档案无论在日常管理还是业务操作方面都发挥着日益重要的作用。电子档案信息安全问题不仅关乎个人隐私的保护，更关乎国家的安全与社会的稳定。所以开展电子档案信息安全风险评估和制定行之有效的防范策略具有十分重要意义。文章首先论述电子档案信息安全问题的意义，然后对风险评估方法进行介绍，主要包括评估流程，评估工具和评估技术，评估标准和指标体系等。基于此，本文提出了一系列针对电子档案信息安全的预防策略，这些策略覆盖了技术、管理、法律政策，以及教育培训和意识提升这四个方面。这些综合措施可以对电子档案信息安全起到多层次保护作用，保证信息资源完整，可用，保密。

关键词：电子档案；信息安全；风险评估；防范策略；技术措施

【DOI】10.12252/j.issn.2096-6261.2023.09.193

引言

数字化时代下，电子档案已经成为信息管理中的一个重要环节，电子档案的信息安全问题也得到了人们的高度重视。信息安全威胁不仅会造成个人隐私泄漏，而且会危及企业商业秘密与国家安全利益。所以如何对电子档案信息安全风险进行评估与处理已成为亟待解决的课题。文章将对电子档案信息安全风险评估方法进行深入探究，基于此提出有针对性防范策略，其目的是为电子档案信息安全防护工作提供综合解决框架。

一、电子档案信息安全的重要性

在当今社会，电子档案已经成为信息存储和传递的主要形式。这些档案往往包含着大量敏感数据，如个人身份信息、商业机密以及国家重要资料等。电子档案信息安全的重要性体现在多个层面，不仅关乎个人隐私的保护，也直接影响到企业运营的稳定性和国家安全的牢固性。保护个人隐私是电子档案信息安全的首要考虑。随着互联网技术的发展，个人信息更容易被非法获取和滥用。如果电子档案的安全得不到充分保障，个人信息泄漏的后果可能是灾难性的，包括身份盗窃、财产损失乃至个人声誉的严重损害。从企业角度来看，电子档案常常包含了企业的核心商业秘密和客户数据。信息安全的漏洞可能导致竞争对手窃取商业机密，或是黑客通过勒索软件进行敲诈，这些都可能导致企业遭受重大财务损失，甚至影响企业的长期生存。对于国家安全而言，电子档案的安全尤为重要。政府部门和关键基础设施运营商管理着大量关乎国家安全的敏感数据。这些数据如果被敌对国家或恐怖分子获取，可能对国家安全构成直接威胁。此外，随着法律法规的完善与国际合作的加强，电子档案的信息安全已经成为国际社会共同关注的问题。遵守法律规定，执行国际标准，不仅是企业社会责任的体现，也是维护国际形象和参与国际竞争的需要。因此，保障电子档案的信息安全是一个多维度的任务，涉及技术、法律、经济和政策等诸多方面。

二、电子档案信息安全风险评估方法

1.风险评估流程

开展电子档案信息安全风险评估过程具有系统性和动态性，涉及潜在威胁识别，风险分析和预防措施决策等。这一进程的起点是建立评价的类别和对象。各机构必须清楚地了解哪些电子档案有必要进行评价、评价的首要目的何在、期望通过评价达到何种结果。清楚了这些重点，才能给风险评估指明方向，突出重点。然后就有必要对风险进行识别。现阶段，该小组将收集与电子档案系统有关的一切资料，其中包括软硬件，资料，人和环境因素。透过这类资料，我们可以找出各种可能威胁档案安全的因素，其中可能有技术缺陷，操作失误，内在恶意行为或是外在攻击。在确定了潜在威胁之后，下一步就是进行风险分析。现阶段，各组织有必要对每个所确定威胁的潜在影响范围和概率进行评估。其影响程度可通过对业务连续性，财务和声誉的影响程度进行评价；并对其发生概率需根据历史数据，安全事件记录和业内其他机构的工作经验进行综合评判。后为风险评价，这一环节通过对风险分析结果和组织风险承受能力进行对比分析，判断出哪些风险可被接受、哪些风险需重点关注。在进行评估时，有必要对风险大小进行度量，并由组织建立风险准则来确定风险处理优先级。最后是风险处理，这个步骤需要组织建立应对策略来减少，转移，规避或者接受在评估期间所识别出来的风险。风险处理策略选择一般是建立在成本效益分析基础

上，以保证资源发挥最大效益。与此同时，还需要对风险评估流程进行定期的重新审查和更新，以确保风险评估流程跟上目前的威胁环境。整个风险评估流程能否有效实施取决于组织内明确的沟通机制以及决策过程。这就需要从高层管理直至基层操作中的每个成员都能深刻理解风险评估的意义，并且在自己的工作岗位中主动参与过程。

2.风险评估工具与技术

在电子档案信息安全风险评估领域中，大量工具和技术的使用是有效评估得以实现的关键。这些手段与技术的目的是以自动化与标准化方式提高风险评估精度与效益。它们可划分为若干大类，即自动化评估工具，定性和定量分析技术，模拟攻击技术和合规性检查工具。使用自动化评估工具，大大提升评估速度与一致性。这类工具可以迅速扫描海量电子档案并发现潜在安全漏洞。比如漏洞扫描器、侵入检测系统等都能对电子档案系统安全进行不断地监测，及时发现、上报安全弱点。另外，配置管理工具还能保证系统设置与安全最佳实践相一致，避免由于配置错误引发安全事件。在涉及定性与定量分析技术的情况下，风险评估专家通常会依赖多种框架与模型对风险进行评估。定性的分析方法，例如优势、劣势、机会、威胁分析、德尔菲法等，主要是通过专家的建议和经验来识别风险。并进行定量分析，例如故障树分析、事件树分析等，通过数学模型计算出风险出现的可能性及可能产生的效应，从而提供较为准确的风险数据。模拟攻击的方法，如渗透测试和红队模拟演练，都是评估电子档案系统安全性的直接手段。这些技术模拟恶意行为者采取的攻击手段以辨识出系统可能不受重视的破绽。通过这一实战演练，使组织对已有安全措施的效果有了更加明确的了解，从而根据这一情况对安全策略进行相应的调整。最后指出合规性检查工具对于保证电子档案系统与有关法律法规及标准保持一致具有十分重要意义。如信息安全管理系统、数据保护标准合规性检查软件等有助于组织保证其安全措施符合具体行业标准、法规要求。

3.风险评估标准与指标体系

电子档案信息安全风险评价标准和指标体系组成评价工作基础框架。该系统保证风险评估过程与结果的可比性，一致性与可信度。评估的标准通常是基于国家的法律、行业的指导方针以及如ISO/IEC 27001这样的国际信息安全管理准则来制定和执行的。这些准则对评估目的，内容，方法与过程进行了界定，对电子档案信息安全风险评估工作提供了清晰的操作指南与评价规范。指标体系的设置，则更加注重具体评价的操作层面，由一系列量化与定性指标组成，来对电子档案信息安全各方面进行测量。量化指标可包括安全事件频度，系统漏洞个数，响应时间和其他统计数据。但定性指标可能涉及员工安全意识水平，管理流程成熟度，安全文化构建状况。这些指标一起形成多层次，全方位评估体系，使安全风险管理更系统化，量化。制定电子档案信息安全风险评估标准和指标体系时需综合考虑组织业务特性，资产价值以及其安全威胁各因素。比如，对储存着机密信息高值化的电子档案来说，就必须建立更严密的安全控制标准与指标。而且对仅含有公开信息的文件也可相应减少某些规定。在执行风险评估过程中，上述标准与指标既需要能保证电子档案信息安全管理在被控状态下进行，又需要能不断地完善。为实现这一目标，指标体系应包括定期检查与评价安全控制措施的成效，以保证其适应不断变化的环境并有效地应对不断出现的各种威胁与挑战。最后，电子档案信息安全风险评估标准及指标体系须具有灵活性、适应性并能随着技术进步、安全环境的改变不断更新。

三、电子档案信息安全防范策略

1.技术防范措施

技术防范措施对于保护电子档案信息安全具有重要作用，其中涉及了各种先进技术，其目的在于从根本上提高电子档案系统运行的安全性。加密技术作为保护的基石，保证即使数据遭到非法存取，也不容易发生信息泄漏。通过加密存储与传输数据，甚至当数据泄漏时都可以有效地阻止敏感信息内容的破译。另外入侵检测系统、入侵防御系统等的布防，对电子档案系统进行实时监控、攻击防御等。这些系统可以发现异常行为以及可能存在的安全威胁等，以便在袭击发生之前就采取行动以制止或者延缓袭击所造成的后果。防火墙的使用进一步增强了对网络边界的保护，有利于滤除不需要的流量并阻止恶意软件及攻击者对网络的侵害。为解决越来越复杂的安全问题，多因素认证已经成了一种行之有效的用户身份确认方法。它需要用户对敏感信息进行两个或者更多验证因素的获取，大大增加了非授权获取的困难。

2.管理防范措施

管理防范措施则是保障电子档案信息安全又一个至关重要的环节，它们通过建立并实施安全政策，流程与标准增强了组织内安全文化与责任感。信息安全政策在管理防范措施中处于核心地位，界定着组织在信息安全问题上的根本立场与目标，并给员工以清晰的行为准则。安全意识培训对于提升职工信息安全素养至关重要。经常组织工作坊及培训课程，可让雇员认识最新安全威胁及防护方法并加强其辨识及预防能力。同时通过模拟攻击演习及其他实践活动使工作人员能够在真实场景中测试并强化自身安全操作技能。在对员工进行培训的同时，建立行之有效的访问控制政策也是非常关键的。保证访问权限的合理配置，使只有授权用户才能够暴露敏感信息，有利于内部威胁风险最小化。另外，对访问权限要定期审查调整，以便对人员变动或者责任改变做出反应。制订业务连续性计划及灾难恢复计划以确保出现安全事件后组织能迅速作出反应和恢复正常运作。

3.法律与政策防范措施

就电子档案信息安全方面而言，法律及政策防范措施发挥着规范及指导作用。这些举措保证了组织运行与国家法律法规一致，还为应对安全事件提供法律框架。制定适当政策不仅可以促进组织信息安全，而且还可以明确安全事件中的责任和减少法律风险。法律法规一般涵盖数据保护，隐私权保护，知识产权保护以及网络犯罪保护等内容，对个人数据及企业敏感信息的处理具有明确导向作用。根据有关法律规定，企业或机构需要建立一套合乎规定的信息处理流程，其中包括在数据收集，储存，加工，传递及销毁各个环节合规运行。信息安全政策应当体现符合法律要求，并且载有关于违反政策的处罚，以保证雇员知道其职责及其可能产生的结果。组织还必须保证供应商与合作伙伴之间同样符合相应法律与政策要求并以合同与协议进行约束，以维护供应链整体信息安全一致性。

4.教育培训与意识提升

电子档案信息安全离不开教育培训与意识提升。这些举措致力于加强每个雇员的信息安全意识，并保证其能执行安全最佳做法来处理日常事务。通过经常性的教育和培训，雇员可以获得确定并处理安全威胁所需的各种技能。教育和培训项目应该涉及多种安全议题，包括基本密码管理和复杂网络安全策略。这些训练需要有实用性以便雇员能把所学运用到特定情境中。举例说就是教员工怎样辨认钓鱼邮件、恶意软件、遭遇可疑活动时怎样举报。另外，意识提升并不局限于安全操作方面的培训，还应该包含对企业数据保护政策及过程的整体认知。员工应该了解其行为对组织信息安全的影响和维护安全的作用。通过实例教学、情景模拟等手段，使职工对潜在风险有更深入的了解，并采取正确防范措施。强调持续学习也是教育和培训内容之一。信息安全领域在不断向前发展，各种新威胁、新技术不断涌现。因此，各组织应该鼓励雇员不断注意安全方面的最新动向与技巧，并透过出席研讨会，阅读行业报告及在线课程来维持知识更新。

结束语

电子档案信息安全风险评价标准和指标体系组成评价工作基础框架。采用系统风险评估方法能够对潜在风险进行有效地识别与评估，综合防范策略是保障电子档案信息安全工作的重点。需要从技术、管理等方面采取措施，加强法律、政策等方面的支持，不断提高相关工作人员的安全意识和技能，从而为电子档案信息安全构筑一道坚强防线。今后工作应重点关注策略的执行及效果评估等方面，以便持续优化安全保护机制并满足信息技术快速发展的需求。

参考文献

[1]赖永聪.电子文件和电子档案管理中的信息安全问题探讨[J].兰台内外，2022，（31）：49-51.

[2]董珈男.基于信息化档案管理的重要途径[A]2022电脑校园网络论坛论文集[C].中国管理科学研究院教育科学研究所，中国管理科学研究院教育科学研究所，2022：4.

[3]佟丽霞.大数据背景下电子档案管理的创新路径[J].黑龙江档案，2022，（02）：233-235.

[4]龙洋.基于数据转型背景的电子档案信息安全研究[J].兰台内外，2021，（30）：27-28.

[5]刘敏.电子档案开放利用中信息安全保障存在的问题与解决对策[J].黑龙江档案，2021，（03）：20-21.

[6]孔旸.大数据、信息化时代电子档案管理的安全问题研究[J].兰台内外，2020，（20）：1-3.