opentext™

信息治理 — 挑战和解决方案

在这个现代化信息时代，组织要面临两个问题：电子数据泛滥和如何管理所有这些数据。每年，信息的累积速度不断加快，与之相关的问题也不断涌现。海量的电子储存信息 (ESI) 会推动储存成本上升，增加 NetIQ eDiscovery 和合规的成本与风险，降低员工的生产力，增大知识产权遭窃可能性和个人识别信息 (PII) 泄漏机率。

七大信息治理挑战及其解决方案：

以下是公司在信息治理方面面临的七大挑战及其相应的解决方案。

1. 信息管理

信息管理要求组织能够检索、获取、保护和维护组织内的所有电子和硬拷贝信息。请注意，各个国家特有的数据保留法、大量潜在的数据储存库和众多潜在的数据格式都会使信息管理变得更加复杂，增加信息管理的成本。

在以前，公司会实施企业级内容管理系统，用于储存所有电子数据。但是，ECM 解决方案软件不一定易于使用，用户有多种方法可以绕开规则（比如秘密存档），或者将数据储存在个人设备和储存媒介中，产生数据孤岛。

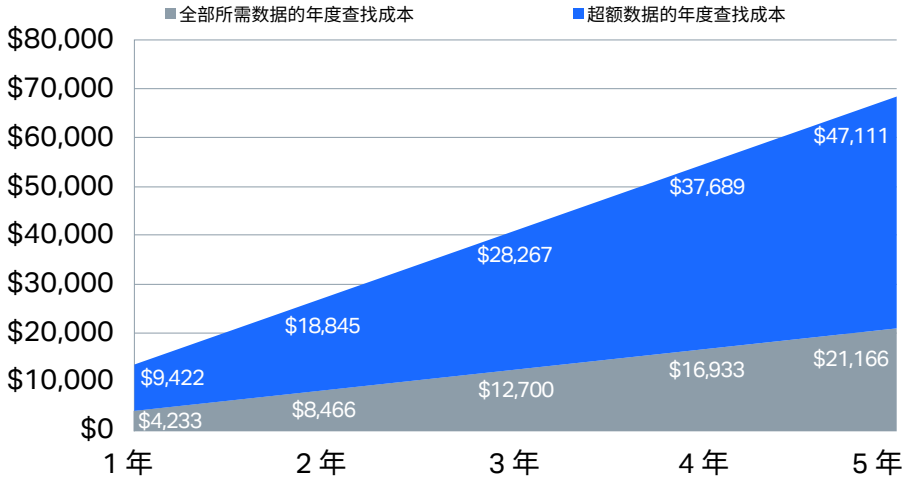
解决方案

为实现真正的企业级信息治理，组织必须实现信息管理自动化。此解决方案让用户不再需要担负数据储存和备份任务，确保贵组织拥有企业级信息管理。

2. NetIQ eDiscovery

如果贵公司无法恰当管理信息，OpenText™ NetIQ eDiscovery 的成本和风险将显著增加。当您面临诉讼时，如果无法在规定时间内找到所需信息，或者无法获得相关信息，成本将会呈指数级增长。为了满足 NetIQ eDiscovery 请求，某些组织倾向于过度收集数据。但是这样做会增加律师费，因为律师必须查看收集到的所有数据，以判断哪些数据与诉讼相关。

每位员工的查找成本和估计可节省的开支



过度收集会使辩护成本增加数百万美元，而收集不足又会让您被控毁灭和隐藏证据，甚至还没开始审判就输掉了官司。

解决方案

有效的信息治理计划是降低 NetIQ eDiscovery 成本和风险的关键所在，这意味着在需要的时候，贵组织将能按照合理的期限保留合适的数据。此外，由于贵组织使用了合适的软件，因此 NetIQ eDiscovery 活动将能快速和轻松地开展，而成本也自然会下降。此图表显示了一名员工随着时间推移而增加的取证成本。灰色阴影区显示了出于诉讼或监管目的应予保留的数据或因为具有商业价值应予保留的数据的取证成本 (31%)。图表中的蓝色区域显示在不需要的或无价值的数据上花费的搜索成本。其中的要点是，法律不要求保留的数据或对企业经营不必要的数据可能会产生高昂的 NetIQ eDiscovery 成本。

3. 遵守法规

不管您位于哪个国家/地区，必然都要遵守关于记录保留的某种形式的监管要求，而且这些要求规定了组织必须保存哪些信息和保存多长时间。如同 NetIQ eDiscovery 对信息的约束一样，您应该谨慎处理受到这些监管要求限制的信息，不遵守这些法律可能会受到惩罚和罚款。受合规要求管辖的数据若没有依法管理和保留，可能会触发政府信息请求。这些请求可能会快速变成昂贵的法律诉讼、罚款，甚至招致牢狱之灾。

解决方案

实施一种信息治理软件解决方案，自动储存行业法规要求的电子记录。例如，企业级信息存档解决方案可以直接连接电子通信系统（电子邮件、社交媒体和移动讯息交换）和文件系统。恰当的存档系统还包含搜索工具、发布工具和 NetIQ eDiscovery 工具。这可以确保数据得到自动保存，无须最终用户管理。

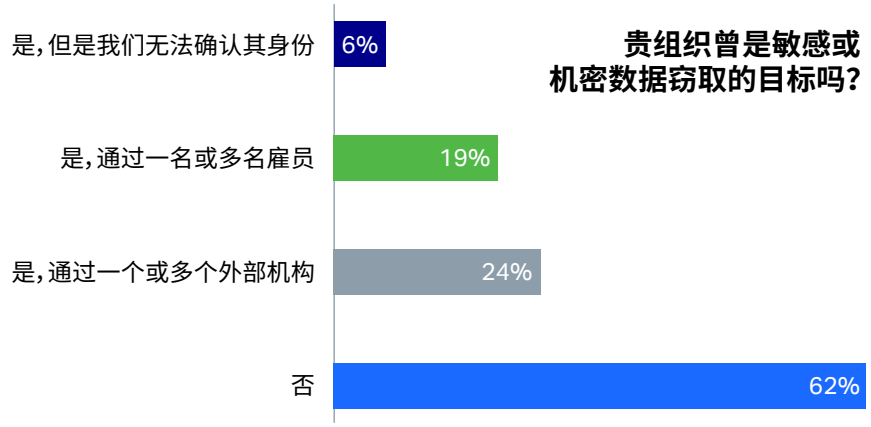
4. 安全和隐私

数据安全和隐私问题与组织面临的合规挑战密切相关。许多政府法规对组织控制的某些类型信息的处理和保留均有要求。至少有两种敏感数据是组织应该竭力控制和保护的，这就是员工和客户的“个人识别信息”(PII) 和“知识产权”(IP)。

疏忽泄漏客户或员工的社会保险号、银行账号、健康信息或税务信息可能会给组织招致官司、罚款、巨额成本和负面报道。知

“我们每月产生 60,000 条外部电子邮件和 300,000 条内部电子邮件，但 Retain 仍然可以满足我们的需要。这笔投资的价值已经兑现，因为我们的 SAN（储存区域网络）存储空间需求降低了 500 GB。我们之前几乎达到 SAN 储存容量。对于我们这种规模的组织来说，这是巨大的节省。此外，我们的用户现在获得了 100% 访问能力。它确实减少了 IT 部门查找电子邮件的时间。”

PAUL RUDIN
网络管理
Grand Bank & Trust of Florida



识产权可能代表组织的巨额投资。若是知识产权因为失窃或疏忽而泄密，则可能会使组织损失数百万（甚至数百亿）美元、失去市场份额、损害股东权益，以及陷入持续的负面报道中。超过三分之一的受访组织表示遭遇过敏感或保密信息的失窃。

解决方案

类似于合规解决方案，组织也必须实施恰当的软件来合理管理和保护信息。贵组织实施的存档解决方案必须符合安全和隐私要求，包括 HIPAA、SOX、FINRA 和其他法规的安全和隐私要求。在选择存档解决方案时，您必须验证该解决方案能否满足这些法规的安全和隐私需求。

5. 储存管理

由于数据增长速度加快，数据量不断增加，IT 部门经常要购买额外的储存资源才能满足需求。即便储存价格不断下降，但是企业信息的数量和增速不断上升，超过了降价的幅度。不断增加的储存量引起的一个问题是，有效备份、查找、管理和使用存档信息的成本随之增加。

解决方案

为了降低储存成本和储存容量，组织必须实现信息管理自动化。自动化可以免去用户处理其电子记录的责任，确保贵组织拥有企业级信息管理。

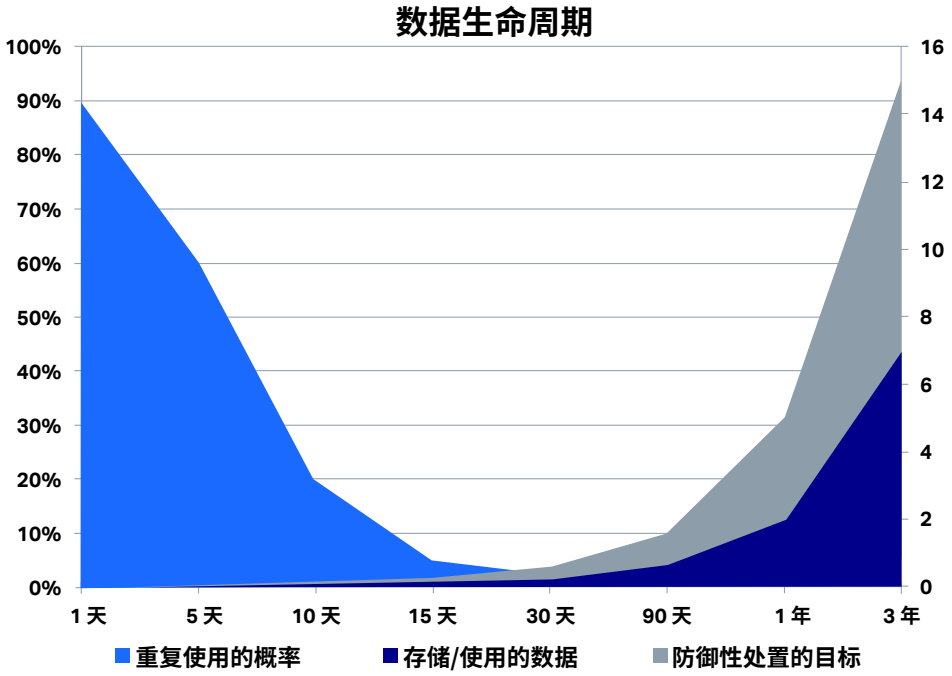
6. 防御性处置

2012 年“合规、治理和监督顾问机构”(CGOC) 开展了一项调查，结果显示组织的数据平均有 1% 要遵从法律保留，5% 要实行政府监管保留，而 25% 有一定的商业价值。依照这种关于数据价值的基本分类，任何组织大约有 69% 的保留数据没有明显的商业价值，可以处理掉而不会产生法律、监管或商业后果。

下图显示了与该理论相关的几个数据点。蓝色阴影区表示随着时间推移重复使用数据的可能性。这是电子邮件讯息的潜在参考或重复使用示例。对大多数员工而言，几乎从来不需要搜索和查看超过两周的电子邮件讯息。因此，15 天过后数据的整体重复使用率快速下降，接近 1%。此图还显示了随着时间推移每位员工的信息增长，以及 CGOC 认为应该保留的信息增长（绿色阴影区）。数据平衡（灰色阴影区）表示可以处置而不会对企业产生负面后果的数据。Osterman 研究发现，只有 46% 的组织实施了防御性处置计划。

解决方案

防御性信息处置有两个关键点。首先，确保处置流程纳入最新的书面策略中。其次，只



处置当前无需按法律保留或不会触发政府请求的任何信息。及时的防御性信息处置可以降低未来招致法律诉讼或触发政府信息请求的风险，降低 NetIQ eDiscovery 审查和储存成本，提高员工的生产力。在计算信息治理计划的投资回报 (ROI) 时，防御性处置是一项重要变量。

7. 生产力

随着组织内的信息日益增多，员工要花越来越多的时间来管理个人工作文件、电子邮件和其他内容。这些时间如果用在员工的实际职能中，应该能产生更好的绩效。事实上，估计每位员工每周要花两至八小时的时间管理这些信息。除了基本的信息管理外，低效的搜索实践和数据重创建 (在找不到存档数据时) 也会妨碍生产力。

解决方案

良好的信息治理实践和解决方案可以为这些做法提供支持，通过减少员工花在信息管理上的时间来提高生产力。

Retain Unified Archiving 解决方案

OpenText™ Retain Unified Archiving 符合所有行业、各种规模的组织对电子通信信息的治理需要。Retain Unified Archiving 能对多个平台所有的电子邮件、社交媒体和移动通信数据等讯息统一存档，以用于案例评估、搜索和 NetIQ eDiscovery，而且它不但可以就地部署，也可以部署在云中。

与我们联系

OpenText 首席执行官
Mark Barrenechea 的博客

如需了解更多信息，请访问
www.microfocus.com/opentext

opentext™