

保护机密数据

报告描述

项目目标

鉴于机密数据的保护是一项重要的业务活动，ESG进行了这项研究，旨在更多地了解当前的做法、挑战以及今后的计划。具体来说，本报告要找到下列问题的答案：

- 问题的定义和范围。
 - 安全专家认为企业有多少数据是机密的？
 - 就以下方面而言，数据存放在哪里：
 - 系统（个人电脑？服务器？主机？存储设备？）
 - 数据管理（文件系统？数据库？非结构化内容？）
 - 用户知道他们有多少份机密数据的副本吗？它们存放在何处？
- 市场动态和采购计划。
 - 机密数据安全解决方案的驱动需求是什么？在什么样的时间范围内？
 - 用户会首先着手解决机密数据保护中的哪些领域？
 - 哪些功能组（IT和业务）负责提高机密数据的安全性？
 - 用户如何制定机密数据保护费用的预算？
- 策略、流程和步骤。
 - 企业有具体的机密数据安全策略和步骤吗？
 - 如果有的话，它们该如何界定、监测和执行？
 - 如果没有，为什么没有呢？
 - 这些策略、流程和步骤的有效性如何？
 - 需要做怎样的变化？
- 技术部署和采购计划。
 - 目前在使用哪些工具？
 - 未来12个月内又将部署哪些工具？
 - 在特定的机密数据安全领域是否有执行以下步骤的趋势：加密、密钥管理、公开密钥基础设施、eDRM或访问控制？
- 特定厂商的信息
 - 在保护用户的机密数据安全方面，哪些厂商或厂商群体提供了最有力的支持？

为了解答这些问题，ESG调查了227位安全、网络、IT和业务方面的专业人员。这些受访者来自北美20多个行业的公共部门及私营企业，其规模从1000名到20000多名员工不等。如需详细资料，请参阅本报告中的“研究方法”和“受访者资料统计”章节。

目录

目录.....	i
插图目录.....	i
表格目录.....	ii
内容概述.....	1
简介.....	2
市场概况.....	2
项目目标.....	3
主要发现总结.....	3
研究方法.....	5
受访者概况.....	6
受访企业（按职责划分）.....	6
受访企业（按 IT 功能划分）.....	6
受访企业（按行业划分）.....	7
受访企业（按年收入划分）.....	7
受访企业（按员工数量划分）.....	8
受访企业（按安全预算划分）.....	8
受访企业（按公开交易状态划分）.....	9
法规遵循义务.....	9
机密信息是普遍存在的.....	11
机密数据安全的驱动因素.....	12
哪里的机密数据存在风险？.....	14
谁是负责保护机密数据？.....	16
C 级领导是有限的.....	16
哪些群体负责机密数据的安全？.....	16
机密数据安全预算的考虑.....	17
机密数据安全的状态.....	19
机密数据和安全技术.....	21
更多具体的机密数据安全技术.....	22
加密.....	24
密钥管理.....	27
机密数据的安全策略和步骤.....	29
机密数据安全策略和步骤的具体问题.....	31
跟踪机密数据的副本.....	33
机密数据的安全和通信.....	34
机密数据的安全和电子文档.....	34

未来的发展方向	37
外包不是一种可供选择的方案	38
密钥管理要求	40
机密数据的集中安全管理所规定的特性	42
厂商评级	45
研究启示	48
IT 行动项目	48
厂商行动项目	49

版权所有©2009。Enterprise Strategy Group, Inc. 保留所有权利。
所有商标和公司名称是其各自公司的财产。本出版物中包含的信息是由 Enterprise Strategy Group (ESG) 认为可靠的来源提供的，但 ESG 不保证其可靠性。本出版物可能包含 ESG 的观点，这些观点随着时间的推移可能会有所改变。本出版物的版权归 ESG 所有。未经 ESG 的明确许可，不得对本出版物的整体或部分以硬拷贝方式、电子方式或其他方式进行复制或将其分发给无权接收它的人，否则都将违反美国版权法并将引起民事损害诉讼，乃至刑事诉讼。