简译版

# 2020 年危害公司数据的五大风险

**非官方中文译文·安天技术公益翻译组 译注**

| 文档信息 | | | |
|---|---|---|---|
| **原文名称** | Five cyber risks that will define 2020 | | |
| **原文作者** | 艾萨克·科恩（Isaac Kohen） | **原文发布日期** | 2020 年 1 月 6 日 |
| **作者简介** | 艾萨克·科恩是 Teramind 公司研发副总裁。 | | |
| **原文发布单位** | Help Net Security | | |
| **原文出处** | https://www.helpnetsecurity.com/2020/01/06/cyber-risks-2020/ | | |
| **译者** | 安天技术公益翻译组 | **校对者** | 安天技术公益翻译组 |
| **分享地址** | 请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块 | | |
| **免责声明** | • 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。<br>• 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。<br>• 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。<br>• 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 | | |

# 2020年危害公司数据的五大风险

艾萨克·科恩

2020年1月6日

对于数据安全而言，2019年是糟糕的一年。从几乎所有指标来看，2019年都是有史以来最糟糕的年份。根据Ponemon Institute发布的《2019年数据泄露成本报告》，数据泄露的平均成本达到392万美元，是有史以来的最高记录。同时，数据泄露的数量也达到历史新高。在2019年上半年，数据泄露事件的数量增加了54%，在此期间有近4000起公开披露的数据泄露事件。2019年，总计有41亿条记录被泄露。

越来越多的消费者和监管机构要求公司对数据泄露负责。2019年10月的一项调查发现，在发生数据泄露事件后，81%的消费者会停止在线与公司交互。这意味着，数据泄露导致的品牌侵蚀和声誉损失，很可能会增加公司数据安全事件的成本。此外，诸如《通用数据保护条例》（GDPR）和《加利福尼亚州消费者隐私法案》（CCPA）之类的监管法规预示着监管力度日益增加。这些法规凸显了2020年数据安全的重要性。

对于那些负责保护公司数据的人员来说，如今广泛的威胁环境经常导致他们精疲力竭。但是，并非所有威胁都是同样严重的，某些威胁更具危害性。

下面，我们将介绍2020年危害公司数据的五大风险。

## 内部人员威胁

网络安全问题通常会让人联想到不法分子在幕后行动，但是实际上，最严重的数据安全威胁之一可能就潜伏在隔壁——员工对企业数据的完整性构成了重大威胁。Verizon《2019年内部人员威胁报告》预计，在所有数据泄露事件中，内部人员威胁占三分之一以上。

内部人员威胁包括故意数据盗窃、意外共享等。可以肯定的是，企业在2020年需要特别关注和应对此类威胁。

借助广泛的员工监控和端点数据丢失防护软件，公司可以防御内部人员威胁。随着数据泄露的后果持续升级，防御内部人员威胁成为确保2020年数据完整性的一项关键措施。

## 网络钓鱼诈骗

尽管企业做出了最大的努力，但是其员工仍会不可避免地收到网络钓鱼邮件，这使公司数据面临风险。不幸的是，攻击者会利用之前窃取的数据，精心制作钓鱼邮件，使这些邮件真假难辨。

在 2020 年，攻击者将采用更多的个性化等诈骗策略（如 HTTPS 加密）。这将促使公司开展安全意识培训，帮助员工识别网络钓鱼邮件。

## 数据库泄露

各种规模的企业都在采用云计算技术。随着绝大多数企业将其业务迁移到云中，数据泄露的可能性也随之增加。这种迁移会对数据安全造成严重的影响。

举例来说，去年 11 月，一位网络安全研究人员在单台服务器上发现了 12 亿条记录，数量之多令人惊讶。这凸显了数据库泄露对数据安全的威胁。

在 2020 年，公司需要明白：技术的进步不能以牺牲数据安全为代价；企业可以设置口令来保护关键公司数据。

## IT 管理员疲乏

网络安全专家面临着一项艰巨的任务。尽管他们每天防御数千次攻击，但是网络犯罪分子和内部攻击者只需成功执行一次攻击即可对公司造成严重的损害。这经常导致网络安全专家疲乏并快速辞职。据估计，有 65%的 IT 专家正在考虑或已经考虑好辞职。

这个问题在公司高层中也普遍存在。在各企业中，首席信息安全官的平均任期为 18 到 24 个月，平均比其他高级主管职位少 4 年。

这种高压力、高辞职率的环境使企业数据面临风险，因为缺乏职位连续性和职位空缺会让攻击者有机可乘。为了解决这些问题，公司需要尽可能优先考虑采用自动化技术。这样，他们可以保护自己的网络免受内部人员和外部威胁的侵扰，使网络安全人员不必持续不断地评估风险。

## 错误地确定优先级

尽管有大量证据表明，数据丢失是公司面临的最大威胁之一。但越来越多的证据表明，

企业高管没有意识到风险。在对澳大利亚 CEO 的一项调查中，只有 6%的 CEO 认识到他们遭遇了数据泄露事件，而 63%的 CISO 注意到发生了数据丢失事件。

同样，只有 26%的 CISO 表示他们的公司已经准备好应对网络威胁，而 44%的 CEO 认为他们的公司能够迅速恢复。由此可见，企业数据安全最严重的威胁之一是：高管不重视。

简而言之，公司及其领导者必须认识到，数据泄露会带来日益严重的后果。

对于数据安全而言，2019 年无疑是糟糕的一年。不幸的是，没有迹象表明 2020 年情况会变好。但是，对于识别并应对最可能的数据安全威胁的公司而言，这可能是一个与众不同的因素，解决这一问题能够帮助它们在 2020 年及以后蓬勃发展。

# 安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

*安天实验室更多信息请访问：* http://www.antiy.com（中文）
http://www.antiy.net（英文）

*安天企业安全公司更多信息请访问：* http://www.antiy.cn

*安天移动安全公司（AVL TEAM）更多信息请访问：* http://www.avlsec.com