ipswitch

Secure. Control. Perform.

IPSWITCH 白皮书

符合数据保护法规的七个步骤

数据保护法规如何应用于外部文件传输

ipswitch

引言

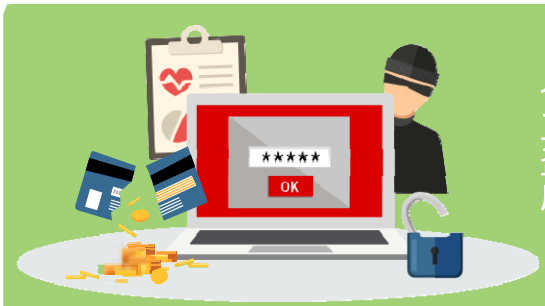
盗取个人资料(PI) 的罪行已为网上罪犯提供了一个庞大的全球黑市市场。由于个人资料包括任何可以辨别个人身份的数据，一些收集密码、信用卡数据、健康数据和地址等数据的公司就成为了网上罪犯的潜在目标。不出所料，自2013 年以来，数据泄露已在全球造成了近 60 亿项数据记录被盗。因此，各国政府都进一步收紧了涉及收集、保存、处理和分享个人资料的相关法例。违反此等法例可导致重罚。

现今，外部传输个人资料已成为各个行业的核心业务流程。零售、运输、金融服务、医疗保健、娱乐、电讯和政府机构等行业的信息科技部门、数据科技和业务流程的外判商均会定期收集、处理和传输个人资料。在保安角度而言，传输中的数据就是身处险境的数据。信息科技团队必须透过工具、科技和外部共享个人资料流程来检视受到攻击的风险。

虽然各国对保护数据的法例各有不同，但一些数据安全控制方法能有助确保符合法规。这份白皮书介绍了七种安全控制方法，确保外部传输数据符合法规。

威胁

个人资料(PI)一般被定义为本身，或与拥有者可取得的其他数据合并时能辨识个人身份的任何数据。对网络罪犯来说，如果能够取得个人资料，那么许多行业便会成为欺诈网站、拒绝服务、勒索软件和持续攻击威胁的目标。



个人资料(PI) 为网络罪犯工具、犯罪专家和被盗的数据提供了一个庞大的黑市市场。

自 2013 年以来，全球数据泄漏已导致 58 亿项数据记录损失。

数据源: Breach Level Index

自 2013 年以来，公开记录的数据泄露已在全球造成超过 58 亿项数据记录损失。损失的数据包括密码、健康记录、账单地址和信用数据等。

没有一个收集和储存个人资料的行业能独善其身，根据 Breach Level Index 报告等数据显示，有 80%的泄露个案是发生在科技、零售、金融和保健行业。如果你的公司需要收集、储存、分享、处理或传输个人资料的话，你便很可能成为攻击的目标。

大部份被盗取的数据都会被传送到黑市兜售，价格按数据的种类和时间(数据在多久前被盗取)而定。每个密码记录的价格可以由 10 美元至 20 美元不等，而最近被盗的信用卡更值 25 美元至 40 美元。

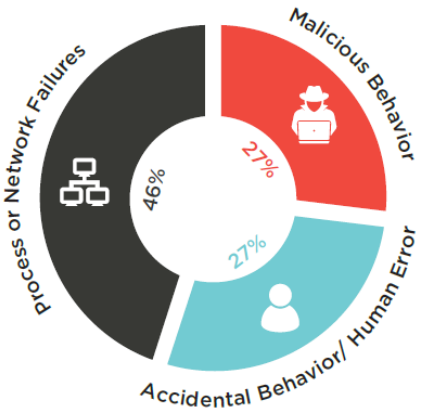
地理上而言，只有很少国家是安全的。美国和欧盟占 2013 年以来被盗数据的74%，另外22 个国家也在同期录得超过250,000 项数据记录损失。当中以中国、韩国、土耳其、日本、墨西哥、加拿大和俄罗斯首当其冲，总共损失了超过 10 亿项数据。

谁是敌人?

谁要为泄露数据负责?传媒往往会令我们以为罪魁祸首是个别国家和网络罪犯，然而，真相并非如此。Ipswitch 最近访问了 255 位信息科技专家，结果显示只有 27%泄露的数据是由「恶意行为」造成。有相同百分比的原因是因为「意外或人为错误」。惊人的是，有46%的数据泄露是因「程序和网络故障」引起的。即是说，我们就是自己的敌人。

真相是，大部份数据泄露都是因为公司或伙伴公司内有人做了不该做的事情。举例而言，数据可以透过没有加密的电邮附件或以网络为基础的文件共享服务传送。此外，你或你的商业伙伴的员工也可能成为大规模的电邮或社交媒体攻击的受害者。

数据泄露的原因



在最近一次电邮诈骗攻击中，一家健康公司的员工被要求输入他们的 EFSS 用户名称和密码 – **60% 的员工遵照了这个做法。**

信息科技组织需特别留意员工和外部伙伴有否使用电邮、未经加密的 FTP 和消费者级的云端服务等不安全的文件共享技术。

当然，有时候大量记录是被网络罪犯的进阶持续威胁盗取，即使如此，部分攻击链通常涉及一个毫无戒心的员工。

你暴露的风险

确定你的公司是否暴露于潜在数据泄露或违反法规风险的第一个步骤，是检查用于与外部交换数据的系统和流程。

默认的文件传输流程

你的主要文件传输流程，尤其是涉及个人资料的，很可能已集中到一小组高度安全的 FTP 服务器。这些服务器使用 SFTP 或 FTPS，以 SSH 或SSL 来确保进行加密传输和身份验证。然而，SFTP / FTPS 仍有限制，容易令你暴露于更多安全漏洞和不合规的风险之中。

FTP 的安全/合规风险

- **缺乏加密:** 如果服务器不是配备 SFTP 或 FTPS 的功能，文件传输将是纯文本（未经加密），在传输过程中很容易便可以透过使用一些简易的技术被盗取。
- **缺乏自动化:** 重复以人手进行文件传输工作会令公司暴露于人为错误的风险当中，导致数据丢失。一些作者已不在公司内任职的文本也是一个风险，因为它们在更改流程或更新保安措施时会被视为已过时。
- **缺乏可视性:** FTP 服务器往往缺少审计师所要求的可视性和日志记录。 日志记录可检视文件有否被篡改，也可以跟踪文件的传输日期、对方收到的日期，以及文件后来有否被删除。
- **缺乏规模:** 公司通常依靠信息科技来开发一系列自制的文本来使其文件传输活动自动化。随着公司的需求越来越多，维护这些文本的规模和复杂性变得更繁重，并且可能造成意想不到的安全漏洞。

特设的文件传输或云端传输

为了遵守数据保护法规，你的公司必须实施监控流程，确保安全处理个人资料。其中一个漏洞是雇员可能会透过电子邮件附件或消费者级的云端文件共享机制等不安全手段，传输受管制的数据。.

电邮和云端文件共享的安全/合规风险

- **加密:** 文件在传输过程中未必会加密。这样明显地违反了大部份数据保护法规。
- **分发:** 不能保证传输的数据只由指定的收件人收到。
- **数据寿命:**在最初传输文件后的几个月内，文件可能仍未被删除而继续存放在系统中。一家保健供货商因为让未加密的数据在互联网上存放两个星期而被罚款 200 万美元。
- **云端的合规性:**即使云端文件共享的宣传声称「合规」，传输数据的公司通常需负责确保传输前、传输期间和传输之后的数据安全。

文件传输的安全控制措施

虽然个人资料保护法规的具体情况因国家而异，但有一套重要的最佳实践安全控制措施可以帮助确保文件传输符合规定。多国政府和行业均广泛采用 ISO/IEC27001 国际标准，因为它确定了许多最佳做法。下表列出了七项与外部文件传输操作有关的最佳实践安全控制措施。

安全需求控制	ISO 27001 ref.	文件传输
1. 合规性	A.18	自动化
2. 通讯安全	A.13	控制和可视性
3. 信息安全政策	A.5	信息
4. 访问控制	A.9	验证
5. 密码学	A.10	密码学
6. 实体和环境安全	A.11	安全架构
7. 业务连续性安全	A.17	故障转移

自动化

常用的文件传输工作流程应该自动化，以减少可能导致数据丢失的人为错误。你的文件传输工具应具备自动转发、错误校正和确认所有数据传输已接收等支持功能。

控制和可视性

传输工作的控制和可视性是重要的安全要求，对确定合规性也是至关重要。你的工具应该能够提供所有文件传输的中央可见性、控制和预先授权。日志应保存在具备防篡改功能的数据库中，以确保可以完整地进行审计跟踪。

信息安全

你使用的技术、工具或流程应确保可以进行文件的完整性检查、接收后删除数据，以及不可否认性 (发送者和接收者都获授权和认证以取得数据)。它们应提供自动审计跟踪，以追踪传输数据的完整性、交付和身份验证。

验证

对用户和管理员的有效认证是一项重要的控制措施。你的文件传输系统应该具有一系列访问控制机制，包括与中央用户目录集成、基于角色的访问控制和单点登录以及多因素认证。

密码学

加密是有限期的。合规性标准通常不允许使用受损的系统。你的系统必须使用强大和最先进的加密机制，并能够安全地选择、分发和保护加密钥。

安全架构

你的系统架构应与现有的安全基础架构和应用程序集成。系统也应确保在 DMZ 内没有未加密的数据，或以网关代理服务器向 DMZ 提供终止身份验证和数据传输的入站请求。

故障转移

许多数据保护法规的一个重要要求是确保业务连续性。此要求旨在出现任何故障、灾难或中断情况时，仍能保护文件传输的机密性、完整性和可用性。自动和安全的故障转移功能可确保文件传输成功或连续重新启动直至完成传输。

ipswitch

Ipswitch® MOVEit 的合规性功能

MOVEit®是一种受控文件传输系统，允许你管理、查看、保护和控制与外部各方的敏感数据交换，确保符合数据保护法规。下表列出了 MOVEit 如何进行七项核心最佳做法，以符合数据保护法规。

个案

Medibank 如何保护敏感数据以符合保健行业的法规

保安要求	MOVEit 受控文件传输
合规性	MOVEit 助你确保文件传输安全、数据时刻受到保护，传输记录还会在销毁之前一段法例要求的期限内，保存在防篡改审计跟踪中。
通讯安全	MOVEit 提供中央可视性、所有文件传输的控制和事前验证，以及加密、追踪和传输不可否认性，包括保护重要项目的审计跟踪。MOVEit 可与现有的安全基础架构、策略和应用程序集成，确保 DMZ 内没有未加密的数据，并可删除外部访问的要求。
信息安全政策	MOVEit 为静止和传输中的文件进行加密，提供不可否认性和进行文件完整性检查。 使用 MOVEit 时， Ipswitch 会为电邮、网站、流动接入和桌面客户端的所有用户提供合规的文件传输接入。
访问控制	MOVEit 提供多种认证机制，包括能与现有系统集成的机制，并有支持用户进行访问管理的功能，包括黑名单和白名单，以及帮助管理员选择最合适的设置以符合安全政策的工具。
密码学	MOVEit 采用强大的加密机制，进行安全选择、分发和保护加密和解密钥，符合国际法律和监管要求。
实体和环境安全	MOVEit 在实施中提供灵活性，确保符合本地实体安全要求。
业务连续性安全	MOVEit 可在任何故障，灾难或中断情况下，保护文件传输的保密性、完整性和可用性。Ipswitch 的故障转移可确保文件传输处理不会间断。

有关 Ipswitch

Ipswitch 以简单的解决方案助你解决复杂的信息科技问题。本公司的软件受到全球数以百万计人士信赖，用于系统、商业伙伴和客户间的文件传输，以及监控网络、应用程序和服务器。Ipswitch 于 1991 年创立，总部位于美国麻省莱辛顿，办事处遍布美国、欧洲和亚洲各地。

详情请浏览 www.ipswitch.com。

Ipswitch MOVEit 殊荣

Network World Asia 2016 读者之选卓越产品奖

100 位来自亚太地区的首席信息官、信息科技总监、数据中心和保安主管获邀在每个组别的决赛者当中挑选优胜者。Ipswitch MOVEit 在安全信息传输组别夺得卓越产品奖。

Frost & Sullivan 2016 产品创新领导奖

在业界最佳实践研究过程中，MOVEit 被发现最能满足客户和行业对安全性，灵活性和可扩展性的重要需求，同时能确保无与伦比的客户体验和易用性。

ipswitch

下载 Ipswitch MOVEit 30 天免费试用 ›