ipswitch

Secure. Control. Perform.

IPSWITCH 白皮书

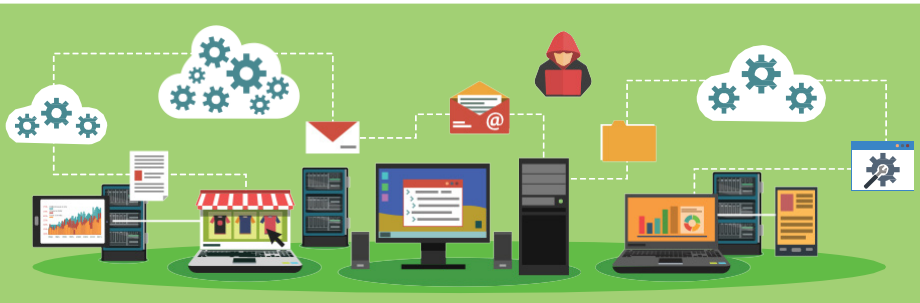
银行与金融服务在安全与法规遵循方面的注意事项

导言

在这个网络犯罪份子和民族国家都在不断刺探着企业安全防御的时代中，数据保护安全措施成了不可或缺的要素。银行和金融服务所收集与储存的数据一旦流入黑市，多半行情不斐。这也让贵组织成了网络攻击的首要目标。

因此，贵组织需要实施能够保护敏感性金融信息以及客户和员工「个人标识信息」(Personally Identifiable Information，PII) 的政策与技术解决方案。社会安全号码、银行帐户信息、地址、贷款月结单以及支付卡卡号之类的数据皆具有敏感性，也属于许多法规的保护范围。若未实施符合州、省籍国家法规 (或产业标准) 等级的安全操作控制，可能必须缴纳巨额罚金，还可能因此名声扫地。

在贵组织的日常作业中，可能也会将大部分的数据传送到安全网络范围外的目的地。定期将数据传送给委外厂商，由对方来代表您为客户提供一部分重要的金融服务，已经成为了现今商业经营的常态。这样的信息交换方式可以让贵组织提供更高水平的服务，同时运用新兴的成长契机获利，然而您同时也必须承担安全漏洞以及数据遭窃、遗失或滥用等问题发生的风险。



敏感数据一旦离开了防火墙，就有可能遭到窃取及滥用。

ipswitch

为保护经济，全球政府皆实施了控管金融信息安全性的法规。光是在过去 3 年内，全球遭窃的资料就有近 60 亿笔之多，因此，全球政府也针对收集、保留、处理以及共享个人信息方面实行更加严厉的规范。

在美国境内营运的银行必须遵守多项涵盖数据保护防御措施或条款的法规。金融服务现代化法案 (Gramm-Leach-Bliley, GLB) 规范收集与披露客户个人金融信息的行为，也规定金融机构必须设计、实施及持续遵守保护这类信息的安全防御措施。沙宾法案 (Sarbanes Oxley) 的稽核条款则规定公开交易组织要能够开放「内部控管与程序」的稽核，同时，凡与具敏感性业务信息相关的所有调阅情形与活动，皆须留下详细的稽核记录。

金融服务组织应该特别留意员工及外部合作伙伴运用电子邮件、未加密 FTP 及消费级云端服务等有安全疑虑之档案共享技术的情形

全球任何一家金融服务公司，只要会收集或储存注明 Visa、Mastercard、American Express 或 Discover 标志的付款信息，同样必须遵守支付卡产业数据安全标准 (Payment Card Industry Data Security Standard, PCI DSS)。个人信息保护法案 (Personal Information Protection Act, PIPA) 规管个人信息 (Personal Information，PI) 或个人标识信息 (Personally Identifiable Information，PII) 的安全，而在全球超过 32 个国家皆实行了某种版本的个人信息保护法。

在美国和其他国家，银行及金融服务组织还必须遵守各州或各省的法规。凡收集、储存或传送有关欧盟居民之客人数据的营业人，还必须遵守一般数据保护规范 (General Data Protection Regulation, GDPR)。

其中许多规范包含重要条款，规定收集与储存具敏感数据的机构及收到或处理该项信息的外部营业人皆须妥善保护此类信息。换句话说，供货商与合作伙伴管理会是法规遵循策略中相当重要的一环。您必须了解对方以及贵组织内部的安全性及法规遵循情形，才能完成正确的风险评估。

最重要的是，未遵守这些法规可能会遭处巨额罚款。

ipswitch

做好资料监管

最近发生了一桩电子邮件诈骗攻击事件，攻击者要求某匿名组织的员工提供自己的 EFSS 用户名称及密码，结果有 60% 的员工配合了这样的要求。

若组织习惯运用企业档案同步与共享 (Enterprise File Sync and Share，EFSS) 及电子邮件等方式与合作伙伴、分公司及客户互传数据，可能会发现这样的做法与数据保护规范背道而驰。这些方式虽然方便，但通常无法达到法规要求的加密、访问控制及稽核记录标准。组织也应该注意一点：即便云端服务供货商宣称其产品或服务「符合」数据保护规范标准，一旦产品遭到滥用或数据遭窃，您必须承担的责任也不会因此减轻。

若仰赖多个 FTP 服务器和必须区分平台的自动化脚本来管理文件传输，随着文件传输过程所用的系统越多，您所面临的攻击风险也越大。IT 团队之所以整合采用单一文件传输系统，其中一个关键因素就是为了减少容易遭受攻击的层面并简化稽核流程。

要遵守法规要求，通常还必须实施严格的访问控制、无时无刻地进行数据加密，同时制作稽核记录。内部安全控管措施也应该要求实行能够保障数据安全的标准化工作流程。为确保遵守法规，银行应淘汰未受管控的文件传输方式，改采安全、可靠且符合规范的信息交换程序，以利确保数据的安全性与周密性。

安全套接字层 (Secure Sockets Layer，SSL) 和安全壳层 (SSH) 这两种常见的安全通讯协议有助于确保数据传输的安全性并提高其稳定度。这两种通讯协议都是针对文件传输加密及相关验证数据而设计的。SSL 和 SSH 强化文件传输安全及可靠性的原理，在于以加密功能来防范透过因特网等开放网络所传输的高风险数据在过程中遭未经授权者擅自浏览及窜改。

无论是在传输过程或静止状态 (保存在储存装置中待开启或下载)，数据保护皆应该持续进行。金融组织应采用市面上功能最强大的密码算法来储存及传输数据。结合 SSL 和 SSH 安全措施与 OpenPGP，就能针对静止中的数据提供多一层的保护。OpenPGP 运用验证用户及数据的密码算法密钥组为储存装置中的档案加密。数据收受方需使用对应的私钥才能将档案解密。

ipswitch

安全的文件传输管理

安全的文件传输管理 (Secure Managed File Transfer) 系统能够以安全、准确、精密控管并详实记录的方式进行外部数据传输，因此有助于因应现阶段及未来可能会实行的各种法律及规管措施。此类系统让金融机构得以在传送数据时收到回条，还能运用广泛的追踪与稽核功能遵守 GLB、PCI DSS、SOX、GDPR 及其他州、省或全国法规。

评估安全的文件传输管理系统或替代方案时，您应该从***机密性、完整性、可用性以及稽核***这四种类别的功来深入了解这些服务的效能优劣。

机密性能够确保唯有获得授权的人员能够在经过核准的前提下使用信息。确保机密性的基础在于验证登入认证信息，以及运用定期失效的帐户及密码管理等功能来施行有力的密码政策。访问控制包括要求所有联机一律支持采用 256 位 AES SSL 加密与 TLS。而这种访问控制等级应强制套用于所有连上贵组织网络基础架构的客户端。

完整性是指确保能够运用完整的 SHA 支持来持续提供所有正确的数据，避免出现漏洞。安全的加密数据传输是确保业务永续发展的重要关键。安全哈希算法能够确保档案不会在传输过程中出现漏洞，也能确保源文件和目的地档案完全一致。不可否认性技术利用加入数字证书管理的方式进行安全传输与数据加密，让数据安全性达到现阶段最高的等级。

可用性可以透过负载平衡和丛集架构达成，这种方式支持自动故障转移及集中储存组态数据，因此能够将数据出现漏洞的机率降到最低。这种方式也有助于防范分布式的拒绝服务攻击。若在解决方案中加入检查点重新启动及加强功能，藉以克服硬件故障或因特网联机中断等问题，将同样有助于确保可用性。

稽核能够提供完整的记录功能及防窜改证据安全措施，因此能够保障记录文件的完整性。基于技术、安全及其他稽核目的，应将所有客户端/服务器的互动与管理措施完整记录下来。

ipswitch

Ipswitch® MOVEit 的法规遵循功能

MOVEit® 是一种安全的文件传输管理系统，能够让您在与外界交换敏感数据时进行管理、检视、保护以及控制，彻底遵守数据保护方面的规范。下表说明 MOVEit 如何一一因应遵守数据保护法规的七项核心最佳实务。

安全规定	MOVEit 控制
法规遵循	MOVEit 有助于保障文件传输安全、全程保护数据，以及将传输记录妥善保存在防窜改的稽核记录中，直到法律规定的期限结束之后再进行安全销毁。
通讯安全	MOVEit 可用于集中查看、控制以及事先授权所有文件传输，还能确保传输方面的加密、记录追踪与不可否认性，包括重大事件的安全稽核记录。MOVEit 的架构基础是整合现有的安全性基础架构、政策与应用程序，确保 DMZ 中没有任何未加密的数据，并且完全不需要透过外部存取。
信息安全政策	MOVEit 无时无刻不加密档案，因此具有不可否认性，而且能够进行档案完整性检查。Ipswitch 提供电子邮件、网络、行动存取以及桌上型客户端，只要搭配 MOVEit 就能让所有使用者进行符合规范的文件传输。
访问控制	MOVEit 提供多样化的验证机制（包括整合现有系统），还有丰富的用户存取管理支持功能（包括黑名单和白名单），同时也提供许多工具，能够协助管理员根据安全政策选择最适当的设定。
密码算法	MOVEit 采用强大的密码算法机制和安全选项、加密和解密密钥散布与保护措施，和国际法规的要求一致。
实体与环境安全	MOVEit 能够在实行方面发挥弹性，有助于确保遵守当地的实体安全规定。
业务永续发展安全	MOVEit 能够在发生故障、灾难或中断问题时全程保障文件传输各阶段的机密性、完整性以及可用性。Ipswitch Failover 能够确保文件传输处理不中断。

关于 Ipswitch

Ipswitch 运用简单的解决方案协助解决复杂的 IT 问题。该公司的软件能够在系统、业务合作伙伴以及客户之间传送档案，也能够监控网络、应用程序及服务器，因此深受全球数百万人士信赖。Ipswitch 成立于 1991 年，总部设于美国麻州莱辛顿市 (Lexington, Massachusetts)，分公司遍布美国、欧洲及亚洲。

如需详细信息，请造访 **www.ipswitch.com**。

ipswitch

下载 Ipswitch MOVEit 30 天免费试用版 ›