数据防护指南

数据防护指南

随着计算机应用的普及，计算机数据安全问题成为了日益突出的问题，特别是在网络环境下，数据的安全问题不仅涉及到系统数据和用户数据遭到逻辑级别或物理级别的损坏威胁，而且涉及到敏感数据通过网络泄漏的威胁。如何保护计算机数据安全已经是重大的战略问题。本技术手册从数据防护现状、数据防护技巧与策略和数据防护应用：电子邮件数据防护三方面着手给大家一些指导意见。

数据防护现状

据 Ponemon Institute 的年度调查显示，数据泄漏的开销已持续增长了五年，到 2009 年为止每条记录已达到 204 美元。这一研究还发现金融服务、通讯和医疗公司会经历更高几率的用户数据泄漏事故。Ponemon 说，这些产业依赖信誉维持业务运转，而数据泄漏会导致信誉的削减。直接接触用户较少的零售商、能源以及媒体公司似乎很少发生大规模的客户数据丢失事件。

- 你的数据是如何泄漏的
- 数据丢失防护工具：防止身份窃取新途径？
- 数据泄露防护：不再只是大公司的事情
- 2009 年数据泄漏给公司造成的损失节节攀升

数据防护技巧与策略

虽然网络通过审计遵从了安全标准，但并不能意味着这样做就能一劳永逸。黑客们了解企业使用的安全方法，甚至其他更多的信息，他们也一直在努力寻找攻破这些安全防护的办法。系统管理员需要跟黑客们一样勤奋，时刻检查和监视他们自己的系统，并且了解最新的攻击技术和安全对策。

- 防止笔记本数据丢失用 DLP 技术还是全盘加密？
- 终端数据丢失防护部署中的五大安全技巧
- 数据泄漏防范：如何跟踪数据和应用程序
- 九个保护商业机密的技巧
- 如何防御黑客窃取信息：员工意识和风险评估策略
- 十步搞定数据泄漏应急预案

应用：电子邮件数据防护

企业面对的一个最大问题是要确保他们知识产权受到充分的保护。通过加密包含公司机密的电子邮件，就不用担心机密信息被拦截以及数据被窃取的可能了，来自竞争对手的风险也会减小。另外，在一个这样的时代，顾客们同样希望自己的私人资料受到保护，而加密通信就能确保客户的私人数据不被窃取。

- 针对 Yahoo 邮箱账户的暴力攻击
- 如何防范对电子邮件帐号的暴力破解？
- 五个步骤成功加密电子邮件

你的数据是如何泄漏的？

不安全的秘密

为什么许多公司不能充分保护他们的商业秘密呢？除了没有完全理解什么是商业秘密以外，他们还有可能没有弄清楚哪些东西是自己的商业秘密。即便搞清楚了，很多公司也没有确定商业秘密的范围、存在的形式（如数字形式，还是纸质文档），以及谁在使用它们。

加利福尼亚州 San Jose 市思科公司的高级安全顾问 Christopher Burgess 问道，“如果你的员工连保护什么都不知道，那么他们如何去保护企业的商业秘密呢？”

另外，一些公司把创新看得比安全重要。思科公司 CHIP 部门的 Parrella 表示，“规模较小的科技公司需要灵活多变，所以他们侧重于产品的开发以及用户服务的执行方面，而不是知识产权的保护”。

就算是世界 500 强的企业采用了适当的知识产权保护措施，商业秘密也还是在不断地泄露。安全过程的弱点、商业流程中固有的漏洞、杂乱的风险管理以及效率低下的培训和宣传计划都会增加这个问题的严重性。

高级管理团队、董事会和高级执行官们经常被误导，错误得认为自己的商业秘密是安全的。这主要是因为他们误解了商业秘密的法律保护，而且安全管理人员处理的日常操作过程也使得他们麻痹大意。

你的数据是怎样泄露的

美国俄亥俄州一家液压泵制造商的一位主管被证实偷窃了公司的商业秘密，并把公司的金融和机密市场规划材料交给了南非的竞争对手。

2006 年，美国的一名肯塔基州的公民被证实策划了偷窃属于 Corning 公司的商业秘密，并将它们进行出售。虽然他只是一个员工，但是这个人偷了 Corning 公司的薄过滤器转换接头液晶显示器玻璃的图纸并把它们卖给了国外的公司。

Duracell 公司的一个员工把畅销产品的敏感数据从公司电脑到下载到自己家里的电脑上面，然后把它们发给了 Duracell 公司的竞争对手。今年早些时候，该员工被判有罪。

一家杂志出版商把它为一本还没出版的杂志制定的价格策略、竞争情报、金融信息和市场计划存储在公共 Web 服务器上的一个隐藏文件里面。但是，由于这个网站的错误配置，这些商业秘密通过 Google 黑客活动暴露给了所有人。

作为协议流程的需要，一家大型科技公司在没有提前签订 NDAs（保密协议）或机密协议的情况下，把详细的规格说明、图纸以及部件信息发送给了潜在的供应商。

在跨国科技公司工作的工程师们，由于个别工程的需要，自己所担任的角色在员工和承包者之间来回变换。就算不考虑子公司设在那些没有强有力知识产权法律的国家这一因素，在每个新工程开始的时候，他们也没有被要求重新签订 NDAs（保密协议）/机密协议。

“当我们跟受害者谈话的时候，我们发现负责研发工程安全的人并不是最高级别的管理人员，所以信息在传达到企业顶级管理人员的过程中，风险也放大了。”

另外，许多企业认为有了像 NDA 和机密协议这样的合同条款，商业秘密被偷窃的风险就会减轻，但是情况根本就不是这样。尽管从诉讼的角度来看这些协议非常重要，但是它们对于防止偷窃并没有起到多大的作用，Schadler 表示，“那些想偷窃商业秘密的人决不会被一个 NDA 束缚住。”

虽然公司可能拥有强有力的、书面的知识产权保护计划，但是它可能会降低员工的工作效率。此外，公司的文化有可能会出现分歧，员工有可能对知识产权的安全规定完全置

之不理。错误的知识产权保护策略阻碍了企业的创造性，而创造性才是让美国公司成为伟大创新者的原因。

原文链接：http://www.searchsecurity.com.cn/showcontent_30112.htm

（作者：Russell Jones and Rena Mears　译者：Sean 来源：TechTarget 中国）

数据丢失防护工具：防止身份窃取新途径？

2006 年，数据盗窃事件在信息安全领域中占据了大半江山； 2007 年，数据盗窃事件的数量只增无减。如果这种态势继续发展下去， 2008 年应该会成为最糟糕的一年。

那些希望防止数据盗窃的企业如果花费了成千上万，而不是数以百万的资金，实施最好的边界安全技术，那么这些努力似乎收效甚微;大量机密信息的泄露继续有增无减，尽管对企业和它们的客户来说后果相当可怕。这激发了安全专业人员对研究新工具的积极性，可以减少他们成为下一个新闻焦点报道的机率。

在过去的几年中，像 McAfee、趋势科技、赛门铁克等众多的信息安全厂商已经在积极研发一套产品，承诺对此将有所帮助。这个产品类别称为数据丢失防护，或 DLP，受到了众多的关注，以至于一些提供反恶意软件和反垃圾邮件的厂商为了进入 DLP 市场，对其业务重点进行调整。举例来说，Clearswift 公司几年前主要的业务重点是反垃圾邮件工具。虽然 Clearswift 公司作为内容安全厂商，其产品线仍包括反垃圾邮件技术，但是它现在将重点放在生产更好的基于网络的数据防护产品。

当软件制造商采用 DLP——过去的安全产品从未采取的方式，努力帮助客户保护数据时，让我们看看这项技术具有怎样的关键特性。

- 保护信息免受意外泄露——企业允许员工获取其最敏感的信息，但是有些员工根本不知道通过互联网发送数据具有内在危险。例如，财务部门的一个新员工，需要将一份机密文件发送到异地的会计师事务所，他可能会将其以电子邮件附件的形式发送，却没有认识到这份文件通过互联网时是以清晰的文本格式发送。确保对所有的机密数据采取适当的措施进行标记，这是企业的责任。DLP 产品确保将机密和关键信息贴上合适的标签，避免员工无意中的泄露。标记数据(tagging)是一个将系统的机密数据分类，并贴上合适标签的过程。由于 DLP 的这项标记功能，从而阻止了员工意外或恶意

试图泄露机密信息。举例来说，一个贴有标签的敏感文件会被禁用通过电子邮件和 IM 进行传送。

- 保护信息免受（来自内部及外部的）恶意窃取——员工的不满情绪仍旧是导致数据窃取的一个重要因素。DLP 的实施可以限制员工传输数据的途径。DLP 也能防止机密数据被复制到 USB 装置、外接式硬盘及 MP3 播放器。
- 符合法规遵从的要求——许多企业需要遵从某些政府的法规，如《萨班斯-奥克斯利法案》（SOX）、《金融服务现代化法案》（GLBA）、《医疗保险可移植性与可信度法案》（HIPAA）或是这三个都需要遵守。今年，在配合法规遵从的要求这一方面，DLP 技术看来将很有可能扮演一个重要角色。例如，HIPAA 要求医护人员对所有的医疗信息保密，而 DLP 策略不仅是保护这些信息的一种手段，而且也是企业证明其采取符合法规遵从的适当步骤的一种方式。

DLP 产品在大型企业网络的应用实施绝非是一件容易的事。大部分的大型企业都有上百台服务器，存有数以千计的目录和文件。需要对这么多的信息做出清理，并决定哪些信息需要被标记，这对任何一个企业来说，都是一项艰巨的任务。但是，企业不同，需要被标记的数据也不同。这个过程绝对不是一刀切的做法。例如，有的组织会选择标记公司的财务信息、商业秘密等，而另一些公司可能不会这样标记。DLP 实施的成功，需要各管理层人员的配合，从而使得数据被适当归类。这样的团队合作才能确保数据标记策略对整个企业来说是合适而正确的。

评估 DLP 时，对其进行测试的主要功能应该包括系统阻止和监控的功能，以及用户阻止和监控的功能。考虑使用基于主机和基于网络的 DLP 产品也很重要，这可以确保没有运行 DLP 接口的系统也能对数据进行保护。

DLP 技术，将成为安全行业新型的防火墙。毕竟，它应用于下一个逻辑层：而该逻辑层是数据存储的位置。不过，在冒险尝试及购买 DLP 技术之前，最好还是对一些厂商的产品进行评估，确保产品的技术能力不会被花哨的营销活动所掩盖。

原文链接：http://www.searchsecurity.com.cn/showcontent_4238.htm

（作者：Peter Giannoulis　译者：Eric　来源：TechTarget 中国）

数据泄露防护：不再只是大公司的事情

监管规则只是在信息被泄露的时候才会起作用，这对于公司来说是个好消息。为什么这样说呢？因为如果你用通用的措施来保护数据，你就可以减少数据泄露的可能性，从而减少因为规则遵从问题而被审计的可能性。

所有公司遵守下面的这些规则都可以改进其安全性：

减少或者排除不必要的法律责任。在数据保护方面，企业应该首先考虑的是删除业务不再需要的数据。这听起来可能有点奇怪，但是从另一角度看，许多公司这样做就能避免对数据进行监管。举个例子，网上的商家可以只存储信用卡购物的交易 ID，从而避免长期存储重要的账户数据。医疗保健公司通过使用一些监管规则没有涉及到的标志符，可以避免存储病人的社会安全号码（Social Security number）。

在整个企业范围来，可以对这类敏感数据进行不同程度的删减。这并不意味着你要删除遵从规则涉及到的所有东西，但至少可以在某些方面减少对敏感数据的使用。这样，在进行下一步“减少数据保护范围”的时候，事情将会变得更简单一些。

减少数据保护的范围。PCI DSS 其中的一个关键要求以及数据保护的一个基本规则是：把受保护的数据限制在一个较小的、精确定义了的范围之内。这种做法不仅让规则遵从变得简单（因为减少了需要执行控制的范围），而且还方便了访问控制、数据移动监控、接触延迟、测试以及安全实际工作中的其他方面。

这一方法的指导思想是：把数据集中在尽可能少的系统以及尽可能小的网络环境中。一旦数据被集中起来，你就可以把对数据的访问限制在特定的用户组和应用程序上。如果可能的话，你应该提供某种机制，当数据驻留在这些集中化的系统上时，能够对数据进行操作。换句话说，你需要避免对数据进行复制或者移动操作。像数据泄露防护软件这样的工具能够监控和限制数据的移动，从而让你的安全控制更加有效。为了进一步约束网络环境，请使用可以把连接限制在特殊地址或者地区范围内的防火墙。最后，请监视所有的数

据访问和数据移动（甚至需要在本环境内进行）。这样做可以确保只有经过授权的人才能接触到数据，而且还有助于符合监管要求。

只共享你必须要共享的数据。现在，很少有公司进行独立的商业运作，绝大多数都会通过各种不同的方式与其他的服务提供商开展合作。不幸的是，与合作厂商共享数据会让数据保护变得复杂起来，因为协作会增加额外的规则遵从。举个例子，美国马萨诸塞州的PCI DSS以及医疗电子交换法案等规则，都要求企业需要对自己的合作伙伴在共享数据的安全事务方面进行评估。这个过程可能会非常的昂贵，所以最好避免这项工作。借用我们先前讨论中的一个想法：如果可能的话，请避免与别人共享数据。

在跟合作伙伴共享敏感信息之前，比较谨慎的做法是对需要共享的信息进行分析，然后用其他类型的标识符进行替换。比如，用你能够映射到实际数据的符号或者ID去代替真正的账号，用类似的伪装数据代替帐户ID等。

就算你不能排除所有的敏感信息，你也能够通过移除不必要的数据以及把数据映射到其他方面来减少数据泄露的可能性。如果经过分析，你还是需要共享伪装数据和映射数据，那么请最好了解一下合作伙伴对这些数据的重视程度。

了解你的合作伙伴。正如我们前面讨论的那样，所有最新的规则都要求你对委托处理数据保护的企业进行评估。幸运的是，对于处理支付卡数据的企业来说，已经有PCI DSS规定了企业必须遵守的标准和一系列的评估程序，而其他的监管规则目前还没有这么明确的规定。

有的企业已在自己开展评估工作了，有的企业则雇佣顾问，还有的企业是让第三方机构来做评估和审计。不管是自己做评估，还是请第三方来评估，你都应该确保这些评估工作满足以下的要求：

1. 按照你的规则遵从要求执行

2. 在影响到你数据的工作和环境框架内进行

3.每年进行一次

如果你关心的是对机密身份数据进行保护，那么遵守这些规则可以让你不必接受关于可用性和操作的 SAS 70 审计。

对你的员工进行培训。虽然数据共享会带来威胁，但是数据泄露最常见的原因却是人为的过失。监管规则要求你确保员工能够意识到他们在信息保护方面的责任。这意味着他们需要理解安全政策、使用复杂的密码、保护设定的密码，以及避免通过不安全的复制、传输或者存储导致数据泄露。

保护你的便携式设备。马萨诸塞州的监管规则首次针对“便携式设备”进行监管。然而，不管你的公司是否需要遵守 201 CMR 17.00，你都应该采取措施来保护存储在容易丢失或者被偷窃的设备或者媒介上的数据。这意味着你需要保护笔记本电脑、U 盘、移动硬盘以及所有能够移动的存储媒介（包括备份磁带。）

对任何一个领域提供详细的指导意见都需要很长的篇幅。本章因篇幅限制，所以不能说的太详细。但是，以下列出的一些经验值得企业借鉴：

1. 书面写出政策，明确地规定哪些类型的数据能够存储在可移动设备或者便携系统上，而哪些不可以。

2. 指定存储敏感数据的具体设备（对 U 盘、移动硬盘等进行标记）

3. 在所有的笔记本电脑和有关的移动存储媒介上采用文件加密系统。

4. 跟踪敏感数据的存储媒介。

5. 开发一种媒介处理程序，确保不再使用的存储设备不会落入坏人之手。

6. 对用来备份的设备进行加密处理，或者进行非常严格的控制。

对数据保护的监管规则和相关合同的遵守，已经从金融和医疗保健机构扩展到所有的公司。然而，这些新的要求不应该引起企业的恐慌。理解数据泄露的风险、需要承担的责任，以及采取谨慎的措施来规避这些风险，对于企业来说应该提上日程了。通过遵守一些很直观的规则（比如本文所列出的这些），一个企业就可以在很大程度上减少数据泄露所带来的风险，而且还遵守了目前和将来的监管规则。

原文链接：http://www.searchsecurity.com.cn/showcontent_29887.htm

（作者：Richard E. Mackey　译者：Sean　来源：TechTarget 中国）

2009年数据泄漏给公司造成的损失节节攀升

据Ponemon Institute公司的年度调查显示，数据泄漏的开销已持续增长了五年，到2009年为止每条记录已达到204美元，但有一些因素包括数据泄漏服务使用的增加以及处理以前的数据泄漏事件而积累的经验正逐渐减缓费用的增加。

Ponemon Institute LLC.采访了45家公司，其中的许多公司已发生过多次数据泄漏事件，数据泄漏的的平均开销从2008年的665万美元上升到2009年的675万美元。“数据泄漏开销第五次年度研讨会”由加密厂商PGP Corp.提供资金赞助，此次研讨会统计了因事故导致业务流失的公司数据泄漏年度开销；将数据泄漏通知到用户和有关当局的开销；司法费用、咨询公司费用以及新的技术投资和员工教育开销。

统计的45家公司中，最昂贵的数据泄漏事件涉及到100,000条客户记录，处理开销达到3100万美元。

这一机构的主席兼创始人Larry Ponemon说：“事实上，没有能真正避免数据泄漏方法；这些事件还会继续发生。好消息是，公司在处理数据泄漏事件时越来越有经验，这会使成本得以降低。”

Ponemon调查中采访的公司有82%通报过不止一次的数据泄漏事件。在先前的数据泄漏事件中积累的经验有助于公司更好地管理事故发生后的善后工作。第一次发生数据泄漏事件的受害者的人均开销是228美元，而经历过两到三次事故后的公司的开销则降为198美元。

Ponemon说：“那些过去经历过数据泄漏事件的公司不会行事鲁莽，他们不会做出唐突的决定，而且他们有时还会雇佣顾问来帮助处理事故响应。”

那些很快通知潜在受害者的公司通常比那些响应迟缓的公司经历过更高级别的数据泄漏事件，并且会精确统计出有多少客户遭受到袭击。

与此同时，这一研究发现许多泄漏事件的发生与这些因素相关：笔记本和 USB 占 40%，系统错误和账户结算表混淆占 36%。Ponemon 说：“恶意攻击占所有攻击事件的约 24%。但导致数据泄漏事件的最大问题也许出在第三方厂商和公司合作伙伴（例如承包商和咨询顾问）身上。”和那些错误有关的数据泄漏事件占公司调查结果的 42%。

Ponemon 说，和以往不同的是，更多的钱被用在了法律防御上。尽管许多集体诉讼被法院拒绝受理，但许多公司还是在壮大司法团队以抗击事故索赔。

Ponemon 说：“一旦法院挑战成功，问题就将接踵而来。”

这一研究发现金融服务、通讯和医疗公司会经历更高几率的用户数据泄漏事故。Ponemon 说，这些产业依赖信誉维持业务运转，而数据泄漏会导致信誉的削减。直接接触用户较少的零售商、能源以及媒体公司似乎很少发生大规模的客户数据丢失事件。例如，2007 年 TJX Cos.在其 T.J. Max 和其他的零售点发生了大量的数据泄漏事故，然而不到一年的时间就出现了转机，它在全球经济衰退时期获取了连续的利益回报，他们获取了用户的赞赏，并依靠折扣来吸引用户。

Ponemon 说：“如果处理得当，公司就将从事故中得以幸存。必须采取纵深防御的方式来做好安全工作并维护好安全环境；不能因为你会幸存下来就将你或你的客户置于数据泄漏的风险之中。”

原文链接：http://www.searchsecurity.com.cn/showcontent_31271.htm

（作者：Robert Westervelt　译者：唐波　来源：TechTarget 中国）

防止笔记本数据丢失用 DLP 技术还是全盘加密？

问：我有一个关于风险优先级的问题。我们让信息管理人员在他们的笔记本电脑上管理敏感数据，但最近我们遇到了这样一件事情，一名雇员因泄漏数据而被抓捕（他随后被解雇）。我想在我们所有管理人员的笔记本电脑上部署一个数据丢失防护（DLP）产品（防止潜在的数据泄漏）、全磁盘加密和远程擦除软件软件，但所获得的资金只允许部署一个产品。你有什么好的建议吗？

答：很好的问题！关于风险优先级存在着很多不同的观点，但我更倾向于用最容易的方法处理更高一级的风险。我的选择是对企业中所有笔记本电脑进行全磁盘加密。

原因有很多，以我在全盘加密方面的经验来看，全盘加密是一个相当强大和成熟的技术。此外，它对用户是透明的，这意味着在运行机器时，用户需要记住几个按钮或选项。相比之下，我对数据丢失防护（DLP）技术的看法是，它们对保护企业电子邮件和其他对外电子信息中的敏感数据很有用，但未必能解决电脑安全问题。

2009 年 4 月，Ponemon Institute 发布了一篇报告：《丢失笔记本电脑的企业风险》。该报告包括了对来自世界各地（包括美国、英国、德国和巴西）的 3100 个信息技术从业人员的 Web 调查结果。

该报告询问受调查者员工通常在什么地方丢失他们的笔记本电脑。以下是调查结果（从高到低显示）：

- 宾馆
- 租用车
- 开会场所
- 机场
- 住所
- 出租车

- 火车或地铁
- 客户办公室

我觉得这个结果很有趣，因为在一周里持笔记本电脑的管理人员可能出现在以上场所中的一个或多个。因此，丢失笔记本电脑的风险很高，这意味着在应对紧急的风险时，全盘加密可能是更容易和更快捷的解决方案。

原文链接：http://www.searchsecurity.com.cn/showcontent_35036.htm

（作者：Ernest Hayden　译者：曾芸芸　来源：TechTarget 中国）

终端数据丢失防护部署中的五大安全技巧

部署终端数据丢失防护可能是所有 DLP(数据丢失防护)项目中最令人恐惧的一步。软件供应商提供的功能集五花八门，恐怕没有哪个组织可以毫无忧虑地加以处理。

这里有五个技巧可以帮你避免常见的隐患，同时成功的保护企业数据：

1. 在静态工作站镜像上测试是非常不错的，但数据丢失防护的大多数问题出现在首次将其部署到使用数据的用户。在你推出部署数据丢失防护解决方案的第一个部门确定一些关键用户，根据需要对他们进行培训，并在测试阶段与他们密切合作。通过关键用户的帮助，可以避免非技术业务部门测试中出现的问题，也可避免部署中没有任何用户反馈的情形发生。

2. 确保你的目录服务器是最新和准确的（这实际适用于任何形式的数据丢失防护部署）。如果你试图根据计算机组而不是用户角色来管理策略，可能会产生策略冲突（特别是当用户发生了变动）。大部分组织将他们的数据丢失防护策略设计成根据用户角色应用不同的策略，例如，财务部门就比客户支持代表有更多的自由来处理财务信息。即使一个计算机组已经映射到一个业务单元或该业务单元中的一个特定用户，在下次更新时可能会破坏该策略。依据用户以及组或者角色要比依据计算机来管理好得多，即使这意味着你首先需要花一些时间对你的目录服务器进行调整。

3. 建立适应用户在你的数据丢失防护网络内和非受控的网络之间变化的策略。例如，在你的网络内有一个数据丢失防护策略检测和阻止你的客户数据库中的信用卡号传输，当终端离开公司网络时，在终端上的策略发生变化，允许正常的使用信用卡。这是完整的数据丢失防护工具和其终端代理诸多特性中的一个，但不是全部。部分文档匹配和数据库指纹策略非常占用内存，远远超过了用户的笔记本和台式机的能力（假如用户在数据丢失防护之外还要处理其他的事务）。切换一个模式匹配策略，例如正则表达将会增加误报，但

会减少对电脑性能的影响。你也可以设置策略切换到监控/警告模式，而不是阻塞模式来进一步减少对用户的影响，虽然安全风险较高。

4.首先关注终端发现和USB保护。在一系列的终端数据丢失防护工具中，发现（查找本地硬盘上的敏感信息）和USB监控/阻塞是最重要的两个功能。帮助跟踪用户在受认可的企业应用程序之外获取敏感信息，和在本地存储或共享敏感信息的行为也是终端数据丢失防护的重要特征。一旦启用终端发现，选择增量扫描（如果你的产品提供了该功能）；没有人希望他们的电脑因为每周三午间的杀毒扫描而突然停止，而每周四又进行数据丢失防护扫描。同时确保你扫描的位置不只是用户的默认文件目录，因为他们很少会把所有文件放在同一个位置。最后，如果你允许用户使用本地的微软Outlook PST文件，确保你的产品可以扫描PST格式的内部去捕获移动到本地存储的邮件。

5.慢慢来，逐步推出代理和策略。在完成你的初步测试后，一个组一个组的推出那些策略来确保产品具有良好适用性，这样以来不会给你的事件响应团队造成太大压力。当用户第一次开始使用数据丢失防护时，几乎每一个DLP客户都会出现大量的策略违反报告，直到用户自我训练到可以更好地管理受保护的信息之时这一情况才会得到缓解。这个过程应该如下：在一个小的用户组中执行一个策略，然后扩大这个策略（和代理安装）持到达到你设定的覆盖范围。一旦第一个策略工作良好，用同样的方式推出第二个策略，虽然你现在不必担心安装新的代理。

虽然这些提示不是部署和管理终端数据丢失防护的所有方面，但仍有助于避免一些最严重的缺陷，并更快的实现你的新工具带来的安全价值。

原文链接：http://www.searchsecurity.com.cn/showcontent_32328.htm

（作者：Rich Mogull　译者：师成　来源：TechTarget 中国）

数据泄漏防范：如何跟踪数据和应用程序

曾入侵 Heartland Payment Systems 公司的三名黑客最近被提起诉讼，该事件也再次强调了严格控制企业数据和访问数据的应用程序的必要性。

在这个众所周知的支付处理公司入侵案件中，入侵者利用 SQL 注入进入 Heartland 公司的服务器。然后，他们安装网络探查器，这些探查器可以捕获在金融交易中使用的银行卡的数据。这种恶意软件能够逃过多种杀毒程序的监测。人们认为，在交易验证过程中，银行卡数据在解密的一瞬间就可以被这些恶意代码所窃取。这次入侵是从 2008 年 5 月开始的，在 Heartland 公司通过遵从 PCI 数据安全标准要求不久之后。

虽然网络通过审计遵从了安全标准，但并不能意味着这样做就能一劳永逸。黑客们了解企业使用的安全方法，甚至其他更多的信息，他们也一直在努力寻找攻破这些安全防护的办法。系统管理员需要跟黑客们一样勤奋，时刻检查和监视他们自己的系统，并且了解最新的攻击技术和安全对策。为此，安全团队的工作不是简单地完成一个检查列表或者通过一个审计就可以了，他们需要做的是在数据的整个生存周期中保护网络资源和数据。在本文中，让我们来看一些跟踪数据和应用程序的方法：

1、映射所在的网络：首先，使用一个工具（比如 Nmap，一款免费的扫描软件）来搜索和记录在网络中运行的设备和应用程序的信息。然后，把扫描的结果跟一个已知的、可接受的安全基准进行比较。定期的扫描能够帮助你了解网络中的内容和用户，以及他们是否应该出现在网络上。对于任何看起来不正常的事务，安全人员都可以对其进行深入的调查，并集中精力处理潜在的不安全领域。

2、监测异常现象：监测进入网络的流量、穿过网络的流量、流出网络的流量是很重要的。要进行远程偷窃数据，黑客不仅要找到数据，还必须有能力得到这些数据。网络行为分析会持续的监测各种流量，并把监视的结果跟一个正常的流量行为基准进行比较和分析。而且，不正常的行为潜在预示出某些错误。举个例子，如果监视到存在与 Heartland 公司付款系统相关的、不正常的收费情况之后，Visa 和 Mastercard 会提醒公司可能出问

题了。也需要定期的对入侵监测系统(IDS)、入侵预防系统(IPS)和防火墙日志进行分析，以便捕获破坏、异常和可疑活动的迹象。

3、知道数据的存储位置： 数据丢失防护技术（比如 Symantec 公司的 DLP 产品系列和 McAfee 公司的 DLP 工具）能帮助确保企业熟知自身的信用卡数据和其他关键数据的存储位置，以及敏感数据的使用方式。这种技术能监视和防止数据复制到可移动存储设备中，该技术正是对付内部攻击的关键。。

数据危害事件可以使一家公司的名誉扫地，并且损失的财产往往比部署优良安全策略的费用要多得多。Heartland 公司的股票自从入侵事件公布以来一直在下跌，公司还面临着法律诉讼和罚款。不能够跟踪运行在网络中的数据或者应用程序，这让企业面对类似的数据泄漏事件时无能为力，会继续长时间忽视数据泄漏问题。

作为最低限度，网络管理员应该使用像 Nmap 这样的工具来建立允许在网络上运行的数据和应用程序的详细目录和基准。此外，在数据使用控制方面，随着网络必须支持的通信信道和便携式驱动的暴增，数据丢失防护产品也逐渐成为必须的安全工具。如果你所在的公司还能够为购买网络行为分析工具（这种工具可以监视流量和检测不正常的活动）腾出预算，那就更好了。网络行为分析不同于即时修复（instant fix），它还是一种不太完善的技术。然而，入侵行为不管多么厉害，都是一种不正常的行为，而这种类型的监测是揭示系统是否被攻破的最佳途径之一。

原文链接：http://www.searchsecurity.com.cn/showcontent_28803.htm

（作者：Michael Cobb 译者：Sean 来源：TechTarget 中国）

九个保护商业机密的技巧

11 月下旬寒冷的一天，在旧金山国际机场，两个男人正准备登上一架飞往东南亚的飞机。他们的行李中有偷窃来的、价值数百万美元的商业秘密。这些偷来的工程设计、操作手册、CD 光盘、软盘和第三方授权的材料可以让国外不怀好意的公司了解最有创新价值的美国公司的秘密，然后在公开的市场上对他们发起竞争。但是，就当这两个人正要登上飞机的时候，被 FBI/计算机黑客行为和知识产权（CHIP）联合调查组当场逮捕。

这听起来像电视剧中的一个片段。然而，这却是发生在 2001 年的真实事件，当时这两个人从硅谷几个非常有名的公司中偷窃了商业秘密，并试图逃离美国。Matt Parrella（美国助理律师、美国公正局 CHIP 部门在 San Jose 市的负责人）指出，虽然在这起案件中罪犯在逃跑的路上被抓获了，但商业秘密的偷盗行为仍呈现上升的趋势，并且偷盗等级也在逐步提高。

他说，“在我们提起诉讼的案件中，偷窃的商业秘密的数量和类型都在增加。三到五年前，我们只是看到有人偷操作手册，但是现在数字版本的图纸、数据资料、制造工艺和源代码也成了偷窃的对象，在这方面的投诉和调查的案件数量也在大幅上升。”

根据美国贸易代表办公室 2006 年出具的一份报告，由于商业秘密被偷盗的缘故，美国企业每年都会损失近 2500 亿美元。联邦法律执行官员指出，大部分偷盗的目标行业集中在生物工程及制药研究、高级材料、非机密武器系统、通信与加密技术、纳米技术和量子计算技术领域。

Randy Sabett（他是华盛顿一家名为 Sonnenschein Nath & Rosenthal LLP 公司的股东，兼公司信息安全和知识产权业务组的成员）指出，各个公司从媒体得到的消息“只是冰山一角，可能还有更多的人没有意识到自己的商业秘密被偷了。”下面归纳出了九条商业机密保护的技巧：

九个保护商业秘密的技巧

1.找到一个你需要的、有威信的公司高层管理人员，以帮助你在企业范围内实行计划。

2.列出公司商业秘密的清单以及它们以什么形式存在的（纸质的、电子版的、没有形成文件的员工知晓的信息）。

3.基于损失的风险性标准，把清单上的内容按商业秘密对公司的价值高低进行排名。为了简化这一处理过程，你可以考虑使用高、中、低三级的方式进行分类。

4.分析这些商业秘密在其整个保密周期中是怎样映射到企业业务程序中的。

5.对商业秘密进行风险评估，然后决定哪些被泄露的可能性大，以及如果这些秘密被泄露的话，会对你的企业造成什么样的影响。

6.基于这一风险评估，你需要清楚的制定出企业范围的数据保护框架文档，该文档包含了在流程和步骤、角色和责任、监视和执行中各自明确的工作，而且员工遵守起来比较容易。

7.进行“缺口分析”，确定你目前保护商业秘密的行动对于数据保护框架来说效果如何。

8.综合使用安全与数据保护政策、对流程和步骤级进行控制、技术控制、物理控制，以及教育和宣传的方法，处理这些缺口问题。

9.建立标准以持续评估保护措施的有效性。

原文链接：http://www.searchsecurity.com.cn/showcontent_30047.htm

（作者：Russell Jones and Rena Mears　译者：Sean　来源：TechTarget中国）

如何防御黑客窃取信息：员工意识和风险评估策略

想想你们公司有的基础设施有多大可能正被不怀好意的黑客盯上。你的基础设施的信息具有多大的价值？是否知道你有多少敏感信息被黑客用小花招给公诸于众了？该怎样阻止黑客窃取你的信息呢？

任何一个真正的黑客的攻击总是从侦察目标开始的。让我们来看看几个比较常见的技术同时也学学如何制止黑客窃取信息。

往往网上散布着的关于你公司的敏感信息会多得让你惊讶——它们就那样等着被人发现。你是否曾经上 IT 论坛搜索你的域名？试试看！公司技术人员很可能会在公共论坛上发布问题和解答，其间会提及公司正在使用的具体设备，也许他们使用的还是他们的工作电子邮件的地址！哎哟！很显然，他们没有意识到危险：那些黑客可能不需要接触你的网络就了解了你在使用哪种类型的防火墙或服务器。

为了避免这种情况，可以开展一个员工意识和公司风险评估政策的培训，从而要求企业用户在公共论坛发布任何信息时使用非工作电子邮件地址。确保你的员工知道公司的名称不应该出现在这些贴子中。这样做并不会影响他们的问题得到解答，然而公司的基础设施的细节却不会让全世界都看到了。

为了了解你的技术人员的信息，另一个黑客会去的地方是在线 IP 地址数据库和网站登记库。 实际上，全球的这类信息被分别保存在四个数据库中。检查 ARIN.net 上的 Whois 数据库，看看在你的公司的域名列表下是否有你公司的技术人员的名字、邮箱、或是电话号码。理想的情况是，你应该只提供了公共的信息，以防止黑客猜测这些人员的身份信息，从而诱使你的员工泄露他们的密码或其他敏感信息。

一个人的垃圾是另一个人的宝藏...是有这么个谚语！“捡垃圾”是一个古老的，肮脏的，但仍效果显著的信息收集技术。攻击者通过分析你不要的信息，寻找社会安全号码，电话号码，用户 ID，IP 地址和密码。鉴于此，员工意识培训计划应得到认真地执

行，以教会员工如何妥善销毁任何可能被利用的信息。您可能认为这是不必要的，但我仍然鼓励你们，特别是 IT 领域的公司，检查每一台网络打印机旁废弃文件的内容。想想如果你发现的东西到黑客手里，你会觉得放心吗？

原文链接：http://www.searchsecurity.com.cn/showcontent_23141.htm

(作者：Vernon Habersetzer　译者：Sean　来源：TechTarget 中国)

十步搞定数据泄漏应急预案

安全专家有充分的理由担心安全信息泄漏，从而制定数据泄漏应急预案。攻击的复杂性和针对性不断增强，被泄漏数据的数量持续上升，有组织的犯罪更加频繁。然而，许多首席信息安全官（CISO）发现，他们无力应对这些攻击。

美国通讯、安全和网络解决方案提供商 Verizon Business 在其《2009 数据泄漏调查报告》中指出，在最近的 10 起数据泄漏事件中，有 9 起本来是可以避免的。虽然这一统计数据本身不值得炫耀，但是它确实表明，在防止未来攻击方面我们可以有所作为。下面我们来讨论一下如何制定和测试数据泄漏应急预案。详细的数据泄漏应急预案不仅可以减少遭受攻击的可能性，而且可以显著降低数据泄漏对企业的影响，并大大节约处理数据泄漏事件的宝贵时间。

下面列出了企业在制定数据泄漏应急预案时应该采取的 10 个高级步骤。只要按照这些步骤执行，你就可以制定出一个可靠的数据泄漏应急预案。

1、利用现有的方法识别和保护敏感数据。

许多企业已经制定了详尽的数据分类方案和数据处理准则，然而这些方案和准则大都过于复杂而难以执行。尽管数据分类很重要，但它也不应成为保护敏感数据的障碍。利用现有的方法设法识别和保护关键领域和敏感数据，这些方法包括业务影响分析（Business Impact Analysis，BIA）、灾难恢复（Disaster Recovery）演习等。可能这些方法已经生成了关于区分和查找敏感数据的大量文档。

2、确定企业的 IT 环境状况，识别潜在的风险领域。

通过仔细观察员工、流程和技术领域并实施高层次风险评估，可以集中精力应对最关键的风险领域。要多与企业内处理敏感数据的人员进行交谈，因为他们知道漏洞所在。另外，还可以考虑聘请外部公司实施风险评估，以帮助企业识别风险最高的领域。对于大型

企业或非传统企业来说，当企业难以确定自己的 IT 环境状况或者企业内部对各个领域的风险等级存在分歧时，聘请外部公司实施风险评估是一个不错的选择。不要一下子面面俱到，而应该首先集中精力应对关键风险领域。

3、制定明确的业务流程，减少意外错误。

大多数的数据泄漏都是由人为失误而不是技术故障引起的。通过制定明确的业务流程并经常对其进行评估，企业可以减少意外的数据泄漏风险。例如，如果每次硬化服务器时都对其配置进行验证，则攻击者就没有什么机会利用服务器上可能导致数据泄漏的安全漏洞。要知道，在数据泄漏应急预案中，这种人为失误可能会造成更大的破坏。

4、制定层次化的防御方法。

层次化的安全防御方法可以大大增加将攻击者拒之门外的可能性。首先，员工是企业信息安全的第一道防线。企业应该对员工进行培训，使其警惕社交工程攻击。企业安全计划中最牢固同时也是最薄弱的环节就是员工。其次，除了提高员工的安全意识，安全专家还应该确保现有的技术能力（例如加密、数据丢失防护等）能够减轻风险。最后，企业还需要提供相应的处理工具，使其他两个层次发挥作用更加容易。例如，如果要求员工加密电子邮件，但又没有加密电子邮件的集成工具，就不会有人遵守这一规定了。

5、扩大数据泄漏应急响应团队的权限。

等待管理层的批准和授权往往会浪费宝贵的响应时间。通过扩大数据泄漏应急响应团队的权限，使其能够当场做出决定又不用担心受到责罚，可以避免这种情况的出现。数据泄漏应急预案还应该与现有的业务连续性或事件处理计划保持一致。这样，数据泄漏应急响应团队就能够及时有效地做出重要决定，协调各个计划处理团队的工作。很显然，管理层应该成为数据泄漏应急处理的主导力量，而不是数据泄漏应急处理的瓶颈。

6、严格测试应急预案，迅速解决发现的问题。

几乎每个企业都编制了一些数据泄漏应急预案文件。然而，据美国技术和市场研究公司 Forrester Research Inc 估计，只有不到 20%的企业定期测试和更新其应急预案。测试的目的是记录“执行项目”和“经验教训”，布置整改措施和后续行动，以确保在数据泄漏事件发生之前妥善解决发现的问题。要确认应急预案符合法律法规的最低要求。否则，企业可能会被视为存在失职行为。

7、制定沟通计划。

与企业的通信、法律和人力资源部门协作，决定如何向下列人员通报数据泄漏事件：a）内部员工；b）公众；c）直接受到数据泄漏事件影响的人员。制定一份准备就绪的沟通计划非常重要，因为当发生数据泄漏事件时，以适当的方式及时通知客户和有关执法机构，可以更容易获得客户和监管机构的谅解。

8、建立内部和外部合作关系。

与取证机构、执法机构以及法律和公共关系公司等建立合作关系，以免当数据泄漏事件发生时手忙脚乱地寻找联系人。事先建立这种合作关系，使企业有充足的时间执行全面的风险评估，并确定适合本企业特定需求的合作伙伴。同样地，作为沟通方案的一部分，还要加强与企业其他部门（例如 IT 运营部门）之间的联系。

9、为应急响应人员提供适当的工具和培训。

应急响应人员需要能够熟练使用各种事件响应工具。如果应急预案是为了在企业内部处理数据泄漏事件，那么就要立刻行动起来，使应急响应人员熟悉取证工具，并掌握明确的证据收集和存储流程。此外，还要确保所有处理数据泄漏事件敏感数据的人员能够妥善处置必要的证据。很多时候，重要的证据都是由于未能正确收集而丢失。

10、将员工作为防止数据泄漏的最后一道防线。

员工不仅是企业信息安全的第一道防线，也是最后一道防线。企业应该教育和培训员工，当数据泄漏应急预案启动时，他们应该如何应对。要使员工在如何处理敏感数据方面

保持清醒的头脑，时常提醒员工，即使没有发生数据泄漏，也不能懈怠和自满。始终保持警觉至关重要。

原文链接：http://www.searchsecurity.com.cn/showcontent_35656.htm

（作者：Khalid Kark　译者：王勇　来源：TechTarget 中国）

针对 Yahoo 邮箱账户的暴力攻击

攻击者愿意做任何事情来劫持邮箱帐户，从而发送垃圾邮件。目前，他们正绕过传统的 Web 登录界面来寻找进入邮箱账户的后门。

这些攻击者已经瞄准了雅虎，并通过自动密码破解脚本成功地破解了雅虎网页服务认证应用程序的账户密码，而这些认证程序被认为是供互联网服务供应商（ISPs）和第三方网页应用使用的。

这一攻击是由网络应用安全联盟分布式开放代理蜜罐项目发现的，该项目由 Breach Security 公司的研究人员负责维护。该蜜罐项目正在跟踪一系列大量成功的、针对雅虎邮箱用户的暴力攻击。

“多年来我们已经知道，高度可见的 Web 界面被暴力攻击之后，垃圾邮件的发送者就会接踵而至，所以多数邮箱服务商会密切留意那些多次登录的情况。“这是一个很好的、标准的做法，”Breach Security 公司的应用安全研究协会的董事 Ryan Barnett 说，“但这并不意味着，终端用户可以在没有访问权限的条件下，尝试登录以激活认证。”

一旦账户被破解，垃圾邮件发送者就可以使用该帐户制作更多的垃圾邮件，或者做出更坏的事情，例如获取账户持有人的个人信息。该方法使垃圾邮件发送者可以知道他们开展恶意活动的地理位置，从而使他们做出更有针对性的垃圾邮件活动。

Barnett 说，暴力攻击的规模很难评估，但这些活动一直没有停止过。黑客不是针对某个用户帐户。因为基于 Web 服务的认证程序没有反自动化的防御功能，攻击者会建立一套自动脚本，从而循环测试常见的密码和可能的用户名。

“雅虎在很多子领域都有这种认证应用，”Barnett 说，“他们拥有数百种这样服务，而攻击者也会到处尝试获取这些认证。”

暴力密码攻击已经存在多年了，它是入侵账户相当笨拙的方法之一。Barnett 说，雅虎对最新的袭击事件已经有了警觉。该搜索引擎巨头使用的是基于 Web 服务的认证程序，可以让用户输入雅虎的密码，从而进入雅虎的第三方合作伙伴的 Web 应用，如流媒体视频播放器。

“我们只能看到他们发送的数据的片段，”Barnett 这样描述正在进行的攻击，“这只是垃圾邮件发送者用来扩大他们恶意活动范围的另一个策略而已。”

Barnett 说，2007 年网络应用安全联盟的分布式开放代理蜜罐项目就已经进入应用阶段。开放的代理服务器能够引诱攻击者通过它来发送信息。与此同时，一种 mod_security 网络应用防火墙（WAF）正在进行监测，并向项目的参与方报告可疑的流量信息。

今年夏天，这个工程的第三阶段开始了。7 月，部署的监视器将由 14 个提高到 60 个。Barnett 表示，该项目还增强了其分析程序的能力。它增加了 Splunk 平台，这是一个日志管理的索引平台，可以进行更强大的搜索和分析。

原文链接：http://www.searchsecurity.com.cn/showcontent_24632.htm

（作者：Robert Westervelt　译者：Sean　来源：TechTarget 中国）

如何防范对电子邮件帐号的暴力破解？

问：为什么现在对电子邮件帐号的暴力破解成为一种流行的攻击技术？这种攻击是如何完成的？那么我们又能做些什么防范措施以在企业级别上去防止这种暴力攻击呢？

答：这个问题问得很好。对于基于网页的电子邮件帐号进行暴力破解变得非常流行，因为这种技术是如此的简单易行。当前的用于暴力猜测密码的工具现在比比皆是，并且只需要掌握很少量的技术就可以很熟练的去应用这些工具，比如像“Brutus”就属于一种这样的工具。你只需要给 Brutus 一个由单词组成的列表（也就是一个词典），这个列表的内容将被作为用户名和密码。Brutus 将从列表中取出任何可能的用户名，密码组合去猜测帐号，直到某一种组合起作用。某些工具可能还会尝试每个密码的一些简单变形（比如”“fluffy8”，“fluffy9”,等等）。这些攻击工具是如此简单以至于一个十几岁的孩子都可以通过简单的点击动作去完成对基于网页的电子邮件帐号的暴力破解的工作。

好消息是我们有许多有效的方法来防止这种针对企业的基于网页的电子邮箱的帐号暴力攻击。也许这当中最直接的策略是使用双因素认证。我们都知道通常有三种形式的认证：

1. 你拥有什么？（比如一张借记卡）

2. 你知道什么？（比如一个密码）

3. 你的东西是什么？（比如你的指纹）

由密码所保护的基于网页的电子邮件帐号就是一种典型的单因素认证机制（即，你知道什么）。由于密码经常会被远程猜测出来或者被盗窃，所以对于限制访问的需求来说这种认证机制是一种非常低安全度的方法。

对于基于网页的电子邮件系统，我建议使用至少两个认证因素，比如使用 RSA 信息安全公司的硬件 SecurID 令牌。这些令牌就如您的手掌大小，便于携带，同时他们能在您每

次登录的时候显示一个不同的登录密码。这个密码永远不会重复，而能达到与某个密码有效期间同步地进行密码猜测的几率是相当的小的。这个令牌（你拥有的）和这个个人身份号码（你知道的）结合起来之后，您只需要如通常那样输入这个个人密码即可。当然，还有很多其他的方式去实现这种双因素认证机制，比如基于软件的认证者或者基于手机的一些认证系统。

另一方面，您也可以通过限制登录尝试的次数来降低网页电子邮件帐号被暴力破解的危险(比如，在一分钟之内三次登录失败将会导致一次十五分钟的系统锁定)。这种方式可以有效地限制一个攻击者进行攻击时的猜测次数。同时，您还需要确保您拥有一个强口令规则，使得在这个规则下的密码都很难通过一般的方法被猜测到进而被检测到帐号信息。最后，如果您的系统存在一个密码复位机制，还需要确保复位密码时所使用的问题的答案的安全，即，它不应该很容易就能够通过一些公开的信息或者社会网络来获得。

原文链接：http://www.searchsecurity.com.cn/showcontent_26993.htm

(作者：Sherri Davidoff　译者：行久　来源：TechTarget 中国)

五个步骤成功加密电子邮件

加密技术已经问世几千年了（自凯撒时期以来），但是仍然很令人费解。

事实上，你每天都在使用加密技术，因为它是驱动安全套接字协议层（SLL）和 HTTP 协议的基本技术。但对于大部分中小型企业（SMB），电子邮件加密术似乎仍然是一个谜，它被认为可以解决所有信息安全问题。然而，让我们先后退一步，来了解一下电子邮件加密术能为你做些什么吧。

首先，中小型企业面对最大的问题之一就是要确保他们知识产权受到充分的保护。通过加密包含公司机密的电子邮件，就不用担心机密信息被拦截以及数据被窃取的可能了，来自竞争对手的风险也会减小。另外，在一个这样的时代，顾客们同样希望自己的私人资料受到保护，而加密通信就能确保客户的私人数据不被窃取。

知识产权保护和隐私考虑都需要面临一个大的无形的问题，那就是合规性。任何与监督管理相关的业务，或者甚至是现在那些接受信用卡(遵循支付卡行业标准)的业务，都需要考虑合规性。当然，电子邮件加密不是针对合规性的万能药，然而它有能力保护关键数据---而这是合规性过程的关键步骤。

为什么邮件加密不是那么普及呢?其实，是源于它的复杂性。从历史记录来看，邮件加密实施起来很复杂，它需要贸易合作伙伴之间的大量的通讯、配置和试验，以确保你加密了的信息，他们可以解密。

此外，我们也没有办法强迫用户去加密敏感信息。IT 管理员曾希望用户能了解怎样加密信息，并且在合适的时候他们能记住加密重要信息。然而，这只是一个希望，大多数组织没能实施。

和大多数技术一样，邮件加密技术在过去几年间已经逐渐发展成熟了。虽然它不简单，但是中小企业开始试验这项技术的成本不再那么高昂了。因为包含能自动执行策略的

密钥服务和邮件网关的服务提供商的出现，大大减少了运行一个加密电子邮件系统需要的成本。

这里有如何加密电子邮件的五个基本步骤：

1. 什么和为什么?

第一步是要确定哪些类型的内容需要被加密。你最好不要与你的法律顾问（或者在律师事务所外）进行这项工作，以确保能确定所有敏感数据，并且创建一个策略来证明保护那些数据的必要。加密内容的类型通常包括客户记录、知识产权、策略文件等等。

2. 谁和哪里?

下一步，确定哪些贸易伙伴将要参与进来，这一点很重要。简单说的话应该是全部。但是在现实中，很多组织在实施过程中都是分阶段进行的，因为加密不是像打开开关然后加密这么简单。要确定你是让用户来决定加密哪些东西（通过计算机软件）还是采用网关的方法自动扫描每一信息来确定它是否需要加以保护。

3. 怎么做?

有很多不同的方式来进行加密。你可以在计算机上直接加密信息或者把加密了的信息存储在一个中转服务器上，然后通过一个网络电子邮件界面来提取信息。你也可以在电子邮件安全网关或者一个单独专用设备上执行加密技术，选取哪种装置取决于你的贸易伙伴的规模和数量。另外，你还可以雇佣一个服务提供商来帮你管理关键服务器或者你自己管理它。只要你确定你需要加密，增值销售商和生产商就一定能帮你做出合适的决定。

4. 什么时候?

把加密邮件同时发送给你的全部贸易伙伴是不可取的。你需要弄清楚哪些合作伙伴可以先着手进行制定执行的细节。随着你不断增添合作伙伴到这个组织，就可以逐渐明确分工了，但是建议你最好能从低处起步然后慢慢实现加密过程。

5. 加以完善

为邮件加密制定完策略和合规性后，就应该把重点放在完善策略（原来用来确定哪些邮件需要加密的策略）上了---任何项目都会有这么一个时期。这个时候可以利用字典和 Heuristics(Heuristics 是一种基于经验的应用程序，它可以通过查找已知资源，常用的文本短语等来获得经验，进而判断电子邮件是否可能有效)以及手工审计加密了的信息（和没加密的信息）的子集，来确保原来的策略得到了执行。

十年前，实现加密邮件需要一大批顾问和大型基础设施。然而那些已经不复存在，但是加密仍然不是一件容易的事。不过有了一个勤奋努力的过程和专门项目小组，电子邮件加密技术将在你的合规性道路上发挥关键作用，而且同时可以帮助你保护知识产权和私人客户数据。

原文链接：http://www.searchsecurity.com.cn/showcontent_2952.htm

（作者：Mike Rothman　来源：TechTarget 中国）