手持和移动设备
安全防护手册

手持和移动设备安全防护手册

现在智能手机和 PDA 的功能越来越强大，越来越受到商务人士的青睐。通过提供实时有效的信息访问连接，移动设备的出现提高了工作效率。尽管如此，事物的出现总是具有两面性的。移动设备在带来机遇的同时，也会由于设备的丢失造成企业机密和个人信息的丢失。还有日益盛行的恶意软件、垃圾邮件和针对移动设备的黑客事件。这些都危及到移动设备的安全，那么作为企业用户该采取哪些保护措施来保护您移动设备的安全呢？本技术手册主要介绍了手持和移动设备所面临的安全威胁，以及保护笔记本电脑和智能手机安全的方法，并总结了移动设备的安全应用策略。

手持和移动设备安全威胁

我最近读到这样一则消息，安全研究人员已经发现一些恶意软件被预装在智能手机上。在过去，智能手机安全威胁专家就曾提到过这一问题，而现在似乎这已经成为了现实，那么各个公司应如何确保所安装（或者是允许接入公司网络）的移动设备平台是没有恶意软件的呢？

- USB 会威胁到内置移动设备的安全吗？
- 下一代安全威胁：智能手机被预装恶意软件

智能手机安全技巧

现在越来越多的商务用户使用高端移动设备，它们具有文字处理、银行帐户认证、网页浏览、收发电子邮件以及其他许多功能。随着远程工作人员的不断增加，当用户不在办公室时，都用这些移动设备来计算电子表格中的数据、读取敏感文件、存储敏感数据。然而，智能手机在企业环境中的大量使用却带来了新的风险，即敏感数据被盗或丢失的潜在危险。

- 怎样防止手机窃听
- 如何为移动智能手机选择加密软件？
- 如何防止 iPhone 上的监听行为：手机管理技巧

笔记本电脑安全全攻略

你有没有想过人们是如何发现或窃取这些不安全笔记本，而其他电脑又是如何攻入这些系统获取敏感信息的呢？我没有采访过任何犯罪人员，但是我斗胆猜测以下他们有自己的工具和技术。不管是多么基础的东西，很多人的笔记本电脑都没简单的密码。电脑工程师都不需要破解代码，而我不会讲这些安全测试技术和这些问题的解决方案。但是那些有密码的电脑呢——那些恶意人士又是如何破入的呢？

- 第一步：笔记本安全问题如何发生
- 第二步：如何攻击笔记本电脑
- 第三步：如何保护笔记本电脑安全
- 第四步：笔记本电脑安全总结
- 逐步恢复被窃的笔记本电脑

移动设备安全应用策略

如今，许多公司的 IT 部门需要做这样一项工作：使工作人员能在掌上电脑（PDAs）或者智能手机这类的无线手持设备上处理商业数据。在理想的情况下，所有的这些设备都是值得信赖的，并且不受恶意软件的干扰。可现实的情况是，许多设备都处于无人管理也没有安全保障的状态，这就成为手机恶意软件感染的理想目标。企业如何才能在这些问题泛滥前，将潜在的风险遏制在萌芽状态呢？

- 移动设备安全策略

- 移动设备网络防御战略
- 智能手机移动设备面临的安全威胁及应对策略
- 移动设备上的应用程序安全
- 如何锁定移动设备 确保企业数据安全

USB 会威胁到内置移动设备的安全吗？

问：使用 USB 会威胁到内置设备的安全性吗？特别是当这些设备是通过 USB 和电脑主机连接的时候，通过使用在电脑主机上运行的应用，这些设备会被入侵吗？

答：确实可以。看一下 USB 设备是如何连接到电脑的，你就明白为什么了。通用串行总线（Universal Serial Bus），也就是通常所说的 USB，它是用于把设备连接到电脑主机上的串行总线标准。一条总线就是在电脑之间或者电脑组件只见个传送数据的一个子系统。作为一个串行总线，USB 一次发送一位的数据。它的创建是为了改善越来越多的想连接到电脑上的即插即用功能。

在刚使用个人电脑的时候，连接新设备是麻烦的事情。那时必须要设置传输器、增加额外的总线或者并口，安装设备驱动并重启，可能是多次。现在有了 USB 这种单一的标准界面接口，这些日子就过去了。USB 设备可以在不需重启电脑或者关闭设备的情况下连接或者断开。当然，它就被广泛地用于连接接口，根据 2008 年的 USB 使用者论坛（USB Implementers Forum）称，目前全球有 20 亿有线 USB 设备。但是，USB 只是连接到电脑主机的接口设备标准。它并不提供任何安全功能来过滤通过连接的数据。在这一方面，这和以太网或者打印机电缆相同；任何通过 USB 连接连到电脑的设备都可以被在电脑上运行的应用访问。所以，假如，如果电脑被恶意软件感染了，这些恶意软件就可以访问通过 USB 线连接到电脑的便携式硬盘上的数据。危险也可以发生在相反的情况，带有自动运行的应用（包括恶意软件）的 U3 USB 设备连接到一台电脑，然后就可以防火电脑主机上的数据或者记录电脑键盘上的所有字符。

为了减轻这种风险，你可以禁用电脑上的所有 USB 端口，但是这不太现实，因为这些端口可能被键盘或者鼠标等设备所使用。如果企业运行的是 Windows 的网络，就可以通过使用 Active Directory（活动目录）控制 USB 设备。不需要使用 USN 设备的个人和团队，就可以通过 Active Directory 组策略，禁止访问 ubstor.pnf 和 ubstor.inf 文件。在 Windows Vista 中，管理员可以允许用户只安装在同意列表上的设备，或者禁止可移动或者使用可移动媒体读写访问设备。还有一些第三方程序可以提供 USB 设备的访问控制范围。

可喜地是我们看到的USB还只是把设备连接到电脑的方法，而不是控制设备行为的方式。为了保护USB设备，你可能需要一些安全措施，当然，这些措施可以被涵盖的策略支持，并可以清楚地和USB设备的恰当使用交流。

原文出处：http://www.searchsecurity.com.cn/showcontent_17372.htm

（作者：Michael Cobb　译者：Tina Guo 来源：TechTarget中国）

下一代安全威胁：智能手机被预装恶意软件

问：我最近读到这样一则消息，安全研究人员已经发现一些恶意软件被预装在智能手机上。在过去，智能手机安全威胁专家就曾提到过这一问题，而现在似乎这已经成为了现实，那么各个公司应如何确保所安装（或者是允许接入公司网络）的移动设备平台是没有恶意软件的呢？

答：智能手机和其他移动设备被预装恶意软件的问题给许多不同的产品线都造成了威胁，并且这种威胁也越来越大。比如在欧洲，送到超市（包括沃尔玛旗下的英国连锁超市Asda）的许多收银台读卡器上就被预装了嗅探器。这些读卡器在生产过程中就已被植入额外的硬件，这样信用卡和借记卡的数据通过移动电话网络传输给巴基斯坦的犯罪分子。根本想不到这些人会从外部进行破坏，因为窃听设备都有三到四盎司重，一些商店最后不得不通过称一下读卡器来检查它们是否被植入窃听设备。

另一个相关的问题是，外国情报机构人员在交易会和展览会上以送“礼物”为由接近商人。这些礼物（如，相机和记忆棒等），已经被发现含有电子木马漏洞，它们可以对用户的计算机进行远程访问。和上述的收银台读卡器的攻击方式一样，我们很难判断该设备是否已经被改装过。

如果产品在被购买之前就已被感染病毒的话，有可能迅速导致消费者对产品和供应商的不信任。任何一家生产或代工 IT 设备的公司，都必须确保这些设备从生产一直到运输和安装的过程中都是绝对安全的。公司还需要采取防止改装的安全措施，或者对产品进行调整以确保产品的完整性。据我所知，有些公司只允许员工使用黑莓手机，因为黑莓手机完全是在墨西哥或加拿大进行生产的，很多人都认为黑莓手机的供应链有着比 iPhone 更严格的控制，因为 iPhone 的零部件来自世界各地。

如果公司里员工有使用移动设备的需求，你可能要考虑使用美国国家安全局的安全移动环境便携式电子设备（SME PED）程序对移动设备进行认证，如 Sectéra Edge。通过此认证的移动设备，会将无线语音通信列为“最高机密”，并将电子邮件和网站访问列为“秘密”的方式，从而对这些服务进行保护。

除非你正在使用一种专门的设备或软件，否则我一直都认为语音呼叫不安全，因此和传真、电子邮件一样，任何时候都不能在移动电话上讨论保密的或敏感的问题。购买移动

设备前，我建议你进行一次测试，看看它是否会试图通过任何可用的网络协议进行异常的连接；你还需要对网络流量进行检查，以确保数据不会被无意地从手机中发送出去。值得庆幸的是，在智能手机和掌上电脑上基于软件进行攻击的数量相对较低，而在智能手机操作系统中所发现的极少数漏洞往往也能迅速得到修复。这可能是由于企业市场中各供应商之间的紧张气氛有所缓和，而设备安全性以及避免受到智能手机恶意软件的攻击目前正逐渐成为人们关注的重点。

原文出处：http://www.searchsecurity.com.cn/showcontent_39261.htm

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

怎样防止手机窃听

问：应该采取那些预防措施来防止手机窃听？

答：这取决与你是谁，以及你认为谁可能监听你。你的手机谈话和通过无线网络进行的活动并不是保密的，重要的是你需要记住手机监听很简单，可以被很多人轻松的截获。因为这些传播媒介本身（大气层）就是为大家所共享的。很久以前，当蜂窝电话网络还是模拟信号的时候，手机窃听是件微不足道的事情，而且厂家还向公众兜售手机信号扫描仪。如今，窃听电话是非法的，而且在系统转变成数字网络后，把截获的射频信号转变成语音非常困难。然而，电信公司、政府和执法部门却可以轻而易举的监听电话，就跟黑客差不多。

法律执行通讯协助法案（Communications Assistance for Law Enforcement Act）于 1994 年生效，于是法律要求通讯载体需安装设备，从而让电子监视变得简单，使得联邦政府机构可以实时的访问电话和网络交流。美国联邦调查局 FBI 有一个很厉害的系统叫做 DCSNet，“它可以让 FBI 探员回放记录，甚至当他们正在被截获的时候（比如 TiVo），创造主窃听档案，给破译人员传送数字记录，利用手机基站实时追踪目标的大致位置，甚至在移动检测车中截获信息流。”（摘自《连线》杂志（Wired Magazine））。美国国家安全局也可以全权访问美国电话公司主要交换点上所有的光纤通讯。

社会上有很多广为流传的报道，即执法部门把用户的手机作为“漫游虫（roving bug）”，远程启动麦克风并从附近区域截获音频，即使手机关机（这可以参考 2006 年关于联邦调查局监视 Genovese 犯罪家族的报道）。E911 法规为实时的手机位置追踪扫清了障碍，允许执法部门在某些时候精确确定用户的位置。

当你不使用手机时，你可以把它放在射频屏蔽袋中，这样能确保它没被用作“漫游虫”或者定位设备。出于这个目的，证据调查设备制造商向公众兜售射频屏蔽网格小袋，有的袋子已经应用在放手机的器件里。

蓝牙系统在设置时的缺陷可以让你周围的人轻松窃听你的谈话，或者远程访问你的电话。Josh Wright 在 YouTube 上对此进行了一个非常好的演示，名字叫做窃听蓝牙耳机。蓝牙设备在处于“可发现”模式时会给窃听者提供敏感信息，他们会通过这些信息来访问你的设备。蓝牙设备工作在配对模式是最容易被入侵的，这是因为为了便于配对，设备之

间会彼此交换敏感的数据，然而这些数据一旦被截获，入侵者就能顺藤摸瓜获得设备的 PIN 密码。所以，为了减少蓝牙窃听所带来的风险，请确保你的设备默认工作中处于非可发现模式下，选一个长的、复杂的 PIN（如果可能的话），不要接受意外的连接请求，只在安全的地方使用蓝牙设备的配对功能。（比如，不在拥挤的运动场所或者咖啡屋里使用蓝牙设备）

除了这些以外，移动设备还很容易受到病毒、蠕虫和间谍软件的侵害，就像台式计算机那样。不过直到现在，已知的入侵还相对较少。但是，随着移动设备的功能变得越来越强大，它们也越来越成为有吸引力的入侵目标。今天，虽然手机恶意软件不是一个迫在眉睫的风险，但是我们也应该提前具备监控能力。

原文出处：http://www.searchsecurity.com.cn/showcontent_27944.htm

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

如何为移动智能手机选择加密软件？

现在越来越多的商务用户使用高端移动设备，它们具有文字处理、银行帐户认证、网页浏览、收发电子邮件以及其他许多功能。随着远程工作人员的不断增加，当用户不在办公室时，都用这些移动设备来计算电子表格中的数据、读取敏感文件、存储敏感数据。

然而，智能手机在企业环境中的大量使用却带来了新的风险，即敏感数据被盗或丢失的潜在危险。一种保护智能手机数据的方法是对手机进行加密。和笔记本电脑加密一样，手机加密产品可以从内置操作系统功能、企业管理工具、第三方软件中获得。

总体而言，商业智能手机加密软件的产品数量仍然很小，可随着越来越多的企业认识到这些设备可能导致的严重安全隐患，加密产品的数量也会快速地增长。企业评估智能手机加密产品时应考虑哪些方面？下面列出了一些最关键的因素：

- 费用：几乎没有公司提供内置加密服务，而通常那些免费或廉价的服务也只对个人提供，几乎没有集中管理功能或政策功能的服务，不能面向企业用户。鉴于这种情况，企业在将来应该为这些产品增加支出，并做出相应的预算。
- 平台支持：大多数企业规定只能使用一个智能手机操作系统，如黑莓的操作系统，但某些特殊的用户（如行政人员或销售团队）却使用不同的设备，像苹果的 iPhone 或 Windows Mobile 手机。因此，在大多数情况下，你应该尽可能的选择一个可以支持多种平台的加密产品。
- 政策重点：针对使用移动设备和保护敏感数据，所有企业都有自己独特的安全需求和政策。一些企业会重点加强认证和密码防护，而其他企业则可能会更多地关注加密。不过，其他企业可能会需要远程数据清除功能以替代诸如加密或认证这样的安全控制。确定企业关于智能手机的安全需求，并由此制定政策重点，不管是在当前还是今后，都将有助于企业选择适合自己的加密产品。
- 集中管理：对智能手机加密技术进行集中管理的政策，以及实时监控每部手机的加密状态，对于具备众多设备的企业而言往往是必要的。此外，在许多不同的规则中都要求的记录和报告，通常只在企业级的管理控制台和产品中才会提供。密钥管理几乎总会被集成到每个企业级的产品中。

接下来，让我们概括一下现在人们所使用的智能手机加密技术的类型。第一类是内置的智能手机加密，它位于手机的操作系统中。几乎没有智能手机具备这种独特的加密技术，即使有也往往只包含有限的加密特性。

目前发现的最强大的智能手机加密技术应用在 Windows Mobile 智能手机上。为保护电子邮件、任务、日历信息以及用户的“我的文档”文件夹，Windows Mobile 提供了可供企业使用的 AES 128 位加密技术。此加密技术同样可以保护存储在安全数字卡（SD cards）上的所有文件，当这些文件加密后，其他任何智能手机都将无法读取。

黑莓是最流行的商务智能手机，它通过黑莓企业服务器（BES）应用程序（一种拥有所有权的独立产品）来提供加密技术。智能手机上的本地文件可以通过集中管理政策（通过激活内容保护功能）来进行加密，也可以通过设备的验证密码进行加密，这些验证密码是利用 AES 加密技术进行安全存储的。

苹果 iPhone 提供了它所形容的“强大的硬件加密技术”，但这名不符实。该功能实际上旨在加强其远程擦除功能，在设备丢失或被盗时消除一切数据。Palm Pre 手机新的 WebOS 没有内置加密技术，但这些仍然使用较旧 PalmOS 的公司可能会发现一些可用的应用程序（包括所有的附加组件）。

大多数智能手机的加密技术来自第三方的商业产品。PGP 公司和 Aiko 解决方案有限公司都为 Windows Mobile 提供了加密产品，而且 PGP 也支持黑莓设备。虽然苹果 iPhone 在个人消费市场非常流行，但因其缺乏管理和安全功能，它在企业中用得较少，并且现今几乎没有真正的企业加密产品适用于此平台。多种加密应用程序，如用户可用的 Firebox、My Eyes Only 和 SMobile ContactCrypt，都只能在本地对数据进行管理。一个确实可以对 iPhone、Windows Mobile 和 Palm 手机进行加密和集中管理的产品是 GuardianEdge 科技公司的智能手机保护，它集成了 Microsoft Exchange，可以对 SD 卡进行加密，还可以提供诸如智能手机防火墙和应用程序控制等额外安全功能。

无论智能手机是在企业环境中还是作为一个独立的设备使用，智能手机加密技术适用于所有的用户。由于这些设备要存储和获取数量越来越大的敏感数据，保护个人和公司数据的需求也变得更加重要。通过对这些设备进行加密，企业通过确保他们的数据安全（无论是手机丢失还是被盗），进一步加强了移动智能手机的安全性。现在最大的问题是：你要如何开始？

对智能手机加密各个方案进行评估时，企业应该做的第一件事情就是确定他们的真正需求是什么，而且这应该是有政策依据的。确保政策明确列出了用户在智能手机平台上可以发送、接收和储存的数据类型，并确保把智能手机的一致类型（consistent type，也可能是模型）作为企业的标准。一旦这些政策得以实施，下一步就是评估数据分类政策和可接受的智能手机使用规范，以作为企业用户每天工作的依据，让他们知道数据保护需求最终是什么样子的。确定哪些用户有智能手机，这些用户可以访问什么类型的数据，然后进行风险评估，以确定这些数据有可能被破坏或丢失的途径。

经过这一过程之后，应该会有助于缩小企业最适合产品类型的范围。其他的一些因素，比如成本、实施的便利性和安全性以及弹性需求，可有助于进一步减小选择的范围。一般来说，确定需要智能手机的任何企业都应确保强大的、值得信赖的加密技术是可能的（例如 AES 128 位或更高位），确保集中管理和政策控制是可用的，而且当智能手机丢失或被盗时，数据可以被清除。

原文出处：http://www.searchsecurity.com.cn/showcontent_37544.htm

（作者：Dave Shackleford　译者：Sean 来源：TechTarget 中国）

如何防止 iPhone 上的监听行为：手机管理技巧

问：我非常担心我们公司的 iPhone 手机会被监视。我们已有规定，不提倡用 iPhone 访问 Web，规定要把内存擦除，要用 PIN 来验证，还要求用户保证他们的手机要在视线范围之内。我们的用户通过 Gmail 发送和接收邮件，但他们通常不使用蓝牙，将其设置为关闭。在这种情况下，第三方是否仍有可能窃听用户的谈话呢？如果真有这种可能的话，我们可以采取哪些防范措施呢？

答：诚然，我希望我的客户都能像你一样认真对待移动设备的安全问题。如果没有密码锁定，那不管谁拿到手机后都能够访问其中的电子邮件和数据。黑客还可以借此机会安装软件，从而窃听电话，甚至在手机待机时记录周围的声音。此外，除非你已经在手机上正确设置了加密，否则不要在不可信的网络里发送明文的登录密码和数据。

Gmail 是一款很优秀的电子邮件，因为它提供了安全的网络连接，而手机在登录并发送电子邮件前必须支持并使用 SSL 连接。

很明显，监听电话是非法的行为，除非你属于情报部门或警察机关，并且得到了这样做的授权。说到 iPhone 和手机上的监听问题，其实最新款智能手机的安全性已经大大超过了以往的手机和模拟信号电话。手机具有的数字技术对于大部分黑客来说都是难以破解的，所以你可以很放心地认为你的电话是安全的。在全球移动通信系统 GSM 网络中，手机与网络间的电话是加密的。在执法时，有非常昂贵（200 000 美元以上）的手机扫描仪，可以对最新款手机进行窃听，但是只有在你参与了严重的刑事犯罪或在谈论极有价值的信息时，别人才有可能会花如此高昂的代价去监听你。

不过，这一切可能也会发生变化。2008 年，安全研究人员展示了最新的技术，这项技术可以大大减少解密所需的时间和费用，因而它可以用于窥探 GSM 网络上的电话和短信。GSM 网络中所使用的是 64 位加密法，人们称之为 A5/1，大概在 10 年前这种加密算法在理论上最先被破解，但一直到现在它还在使用。

安全研究人员所提出的这种设备只需花费大约 1000 美元，在 30 分钟内就能成功破解 GSM 加密。不过如果你想在更宝贵的 30 秒钟之内破解加密，那么你仍需支付约 10 万美元，而 GSM 协会声称，在这种 1000 美元的破解设备面市之前，他们早就布署了更高级的加密算法。

另一种可以利用 iPhone 进行监听的机会出现在跨网打电话的时候，比如说在不同移动网络提供商之间、或者不同国家之间。这些电话将经过各种交换设备和网络，可能会以未加密的数据流形式进行传送。这意味者，电话在任何未加密的一点上都有可能被窃听。

另外别忘了，不管你什么时候开机，你的网络运营商都会知道你所处的地方，精确到一百米左右。这是怎么办到的呢？通过计算各个基站的信号强度，运营商就可以用三角测量（triangulate）知道你的位置并找出你在哪里。

有一些像 CellCrypt 这样的公司提供端到端的加密电话，甚至在不受信的网络上也可以进行安全传输。不过，双方都得在手机上安装一款相同的应用软件。除非您使用的是特制的设备或软件，否则我绝不会认为语音电话是安全的。因此，和传真以及电子邮件一样，不要用电话来讨论机密或敏感的问题，也不要留下涉及到机密的语音信息。你得考虑将要同别人交流的信息有多少价值，然后选择正确的交流方式来分享这些信息。

如果你允许员工使用 iPhone，那么在保障 GSM 网络的安全上我们实际并没有什么可做的，这对其他任何的手机而言都是这样，因此制定一套高强度、可接受的使用规则至关重要。你可以考虑禁止使用未知的接入点，并确保您的邮件服务器被设置为只允许通过 SSL 进行 POP 或 IMAP 访问，从而保证邮件安全地传入传出。Outlook Web Access 或 Lotus Domino Web Access 也是可选用的，因为它们都使用 SSL。同时，你应该强制使用 PIN 号码以及自动锁功能。另外，确保所有手机都在你的视线之内，这一点也很重要。有了物理接触之后，破解 PIN 和加密数据就变得相对更容易了，而远程擦除功能只有在 iPhone 接入手机网络之后才能实施。

此外，iPhone 应用程序商店里还有一些企业管理工具软件，例如 Secure IT Management，但这些工具的效果依赖于用户个人，他们往往需要遵守公司的使用规则，特别是在终端上防止窃听电话这个问题上。敏感的通话不能在公共场合进行，因为这可能会被别人听到。在信息分类策略中，你应该重新强调某些信息所允许使用的交互方式，以防止信息在不经意的谈话中被泄露出去。iPhone 的功能确实很丰富，但随之而来的安全风险不可能完全避免，因此，一切小心为妙。

原文出处：http://www.searchsecurity.com.cn/showcontent_33044.htm

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

第一步：笔记本安全问题如何发生

你有没有想过人们是如何发现和/或窃取这些不安全笔记本，而其他电脑又是如何攻入这些系统获取敏感信息的呢？我没有采访过任何犯罪人员，但是我斗胆猜测以下他们有自己的工具和技术。不管是多么基础的东西，很多人的笔记本电脑都没简单的密码。电脑工程师都不需要破解代码，而我不会讲这些安全测试技术和这些问题的解决方案。但是那些有密码的电脑呢——那些恶意人士又是如何破入的呢？

接触这个问题的做好方法是从恶意的角度看问题。我并不是提倡或者支持犯罪活动。但是，我确实强烈的相信真正保护系统的唯一方法是从犯罪的角度查看安全问题。当说到笔记本黑客活动的时候，你需要运行一些测试查看你可以用多长时间进入系统和你的网络。

已经以完全的权限登录了

电脑系统正在开启的时候就可以被窃取。电量充足的笔记本对这些人来说最方便。不需要中断，然后重新进入—— 他们只需要接受系统并在另外的地方运行，并查看可以收集到什么信息。

一旦他们进入了，任何东西都成了可攻击的对象。很多企业都有这样的政策，任何敏感信息都不能存储在本地硬盘或者移动设备上。正确。我总是看到这样的问题。经常会在个人的电脑上看到各种类型的 Word 处理文档、电子表格文件和其他包含敏感信息的文件。

自己看一下。如果你激活了远程登录并且是本地管理员组的成员，就可以从网络上自己做了。可以在 C:Documents and SettingsAll UsersDesktop and C:Documents and SettingsusernameDesktop 下查看。还可以登录手还在 Outlook 或者其他类型的邮件客户端，查看里面存了什么。用户可能采用邮件作为信息存储库，它就成了敏感信息的金矿。

考虑一下，如果这种数据可以被犯罪分子看到会发生什么呢？所以应该使用简短的屏保时间，要求用户在电脑不适用的时候锁定屏幕，或者在用户离开的时候自动锁定屏幕。

推断密码

犯罪分子的下一步可能是简单的推断登录或者屏保密码——有时和 1-2-3 一样简单。在这种情况下，我们假定电脑是开机的，而且用户使用屏保锁了屏幕。很黑可以输入用户的登录 ID（可能显示上次的登录 ID）作为密码，或者在结尾增加 a 1、感叹号或者“pass”。实际上，这很常见。如果屏保密码不起作用，可以简单的重启系统来查看——可能不需要密码就能登录 Windows.

如果重启了，而且提示你需要 BIOS 开机密码，这就是另一层的防御了，但是绕开也没问题。有很多办法重新设置这些密码。

原文出处：http://www.searchsecurity.com.cn/showcontent_19657.htm

(作者：SearchEnterpriseDesktop.com 译者：Tina Guo 来源：TechTarget 中国)

第二步：如何攻击笔记本电脑

寻找密码

如果黑客已经进入了笔记本电脑，他们就可以查看存储的密码，进入查看其它的敏感信息——特别是存储在 VPN 客户端的可以提供直接进入网络的信。这类信息可以使用类似于 ElcomSoft Ltd.公司的 Proactive System Password Recovery 等的工具找到。它可以恢复登录密码、网络密码、无线加密密钥、拨号/VPN 密码以及其它更多的可以用于攻击的信息。图 1 是 Proactive System Password Recovery 这款工具的界面。

图 1：Proactive System Password Recovery

破解密码

如果你已经做了恰当的事情并要求 Windows 使用 Windows 强制的强大密码登录，你可能会想别人还能用别的什么办法攻入呢。不要担心，还是可以实现。只是简单的密码破解，甚至不需要购买工具就可以做到。我曾经用过一个相对较新的攻击叫做 Ophcrack，它使用 rainbow tables 快速破解 Windows 密码。Ophcrack 有一个可启动的“Live CD”版本，可以不用其它方式访问 Windows 系统就可以使用。所以，考虑一下：犯罪分子可以找到/窃取你的系统，使用 Ophcrack 等工具启动，而后，在几分钟内他就可以获得一个或者更多的 Windows 帐户密码。在这之后就全部结束了。可以自己运行 Ophcrack Live CD，看看可以找到什么。

图 2 显示的是 Ophcrack 的 Windows 版本——Live CD 的 Linux 版本本质上和这个是一样的。

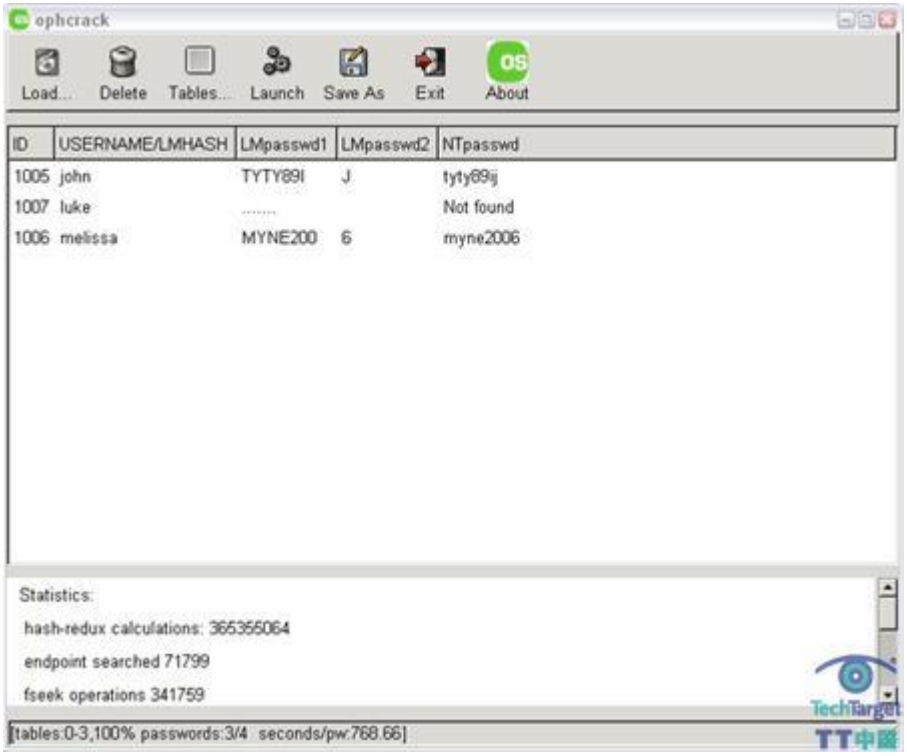

图 2 ：Ophcrack 的 Windows 版本

原文出处：http://www.searchsecurity.com.cn/showcontent_19686.htm

(作者：SearchEnterpriseDesktop.com 译者：Tina Guo 来源：TechTarget 中国)

第三步：如何保护笔记本电脑安全

简单的解决方案

前文已经解释了所有这些笔记本电脑的攻击技术和工具，你可以关闭系统防止恶意事件的发生。可以创建一个加密的“分区”，它基本上是和正常的磁盘一样的文件。但是我并不特别鼓励这么做。这都要归结于你不信任你的用户每次都会把敏感数据存储在安全的分区上。用户会把资料存储在没有保护的桌面上、邮件应用中以及本地的临时目录下。此外，如何有人可以获得笔记本，并向我之前所描述的那样破解各种 Windows 密码，这些加密的分区使用相同密码的几率你认为有多大呢？以我的经验来看，可能性非常大。

很多人都在笔记本电脑上安装了 LoJack 等笔记本电脑跟踪软件，它可以帮助提供恢复功能。问题是在系统恢复的时候，笔记本上的敏感信息也会受到攻击。很好的解决方案——在安全泄漏时就会有点儿晚了。

真正可以防止信息被攻击的安全解决方案（虽然还不是百分百——没有绝对的）是使用全盘加密技术，例如 PGP Whole Disk Encryption、Voltage Security SecureDisk,和 SecurStar DriveCrypt Plus Pack。他们是独立于系统之外的，他们使用强大的加密技术，有些甚至可以集中管理减少管理员的负担。技术被窃笔记本电脑是开机的，只要整个磁盘是加密的，而且屏幕是锁着的，犯罪分子的唯一选择就是重启系统再次攻入。一旦他这么做了，就会提示他输入密码短语，解锁磁盘。只要加密磁盘的密码短语足够强大，犯罪分子就走到死胡同了。还有，要注意 Windows Vista 中的 BitLocker Drive Encryption，以及 Seagate Momentus 磁盘中的内置加密功能。这些技术也很有前景。

切记这些技术的相关策略——不要只信任用户会作合适的事情——这样可以防止电脑上的敏感信息被攻击。当然，在软件许可证和操作成本上都会产生费用（之前和当中）。但是这应该相对于丢失信用卡商业权限来说是更好的选择，向政府法规部分解释为什么你被窃的系统没有被保护，或者通知每个信息被攻击的用户。

原文出处：http://www.searchsecurity.com.cn/showcontent_19742.htm

(作者：SearchEnterpriseDesktop.com　译者：Tina Guo 来源：TechTarget 中国)

第四步：笔记本电脑安全总结

笔记本电脑的安全风险是现实中的人遇到的现实问题，而且如果你——和你的管理层——采用可正确的方法就可以避免。以下是可以保护你的笔记本电脑和其他被窃的电脑的安全的一些办法：

1. 从恶意的角度查看笔记本电脑的漏洞并经常重复。
2. 教育你的用户——一次又一次，直到在他们的脑子里生根——而以下这些想法就像“我需要快点买东西——车里的笔记本应该很安全”以及“我要快点儿去卫生间——咖啡店的其它人可以帮我照看东西”都很危险，最后可能给很多人带来麻烦。
3. 确保屏幕已经通过 CTRL-ALT-DEL 或者屏保已经锁上了。
4. 配置 Windows，在从休眠、待机或者屏保恢复时要求输入密码。
5. 最重要的是，使用强大的密码短语进行全盘加密。

你被窃的系统总是可能被售卖，新的软件可能被重装而且不会产生恶意行为。但是，你应该看一下最糟的情况。假设很多信息被存储在不同的位置，而没有全盘加密和合适的密码以及屏幕锁定技术，就没有办法确定所有的资料总是被保护的。这是任何精明的商业人士都不愿意遇到的风险。

原文出处：http://www.searchsecurity.com.cn/showcontent_19772.htm

(作者： SearchEnterpriseDesktop.com 译者：Tina Guo 来源：TechTarget 中国)

逐步恢复被窃的笔记本电脑

去年年底，一辆停在波士顿城外伍斯特理工学院（Worcester Polytechnic Institute）的学生车里的一台笔记本电脑被盗了。幸运的是，这名学生在购买笔记本电脑的时候，还购买了跟踪软件，这使得校警得以跟踪、锁定了这台电脑的位置。在几个星期之内，这名学生的笔记本电脑就物归原主了，窃贼（连同其它几台盗贼的笔记本电脑）被警方拘留。这起案例中，IT 部门协助警方追缴笔记本电脑的经验，为自适应软件(adaptive software)如何协助追缴笔记本电脑和防止小型电子设备失窃提供了很好的借鉴。

根据 FBI 的调查，每年大约有 200 万台笔记本电脑被盗。更糟的是，只有 2%被追回了。再考虑到笔记本电脑中保存的数据，这就让 IT 部门更加头痛了。这和丢了一个钱包一样，只不过这种情况下钱包可能得有大货车那么大。而且货车里装的还是各种各样的信息，从客户的名字和账单信息到 CEO 的信号卡号。

最容易被追回的电脑就是没被偷走的电脑，所以采取措施预防电脑被偷是明智之举。这里我们列出一些防止笔记本电脑失窃的最好办法：

1. 随时关注电脑的去向;小心驶得万年船。打击盗窃的首要措施就是防止盗窃。公司和员工个人都应该共同承担起这个责任。当笔记本电脑不得不留在桌上时，公司应确保安全线缆(securing cable)可以将该笔记本锁上。不管怎样，员工还是得多留个心眼，注意保管好自己的笔记本电脑。
2. 对笔记本电脑作标记，以区分它的主人。现在已经可以买到这样的物理设备，它能帮助找到笔记本电脑的人把电脑归还给失主。这种装置--通常是贴在电脑外部的一个小块--上面有一个明显的识别号码，在拨打 800 电话寻找失主时可以以此作为依据，800 号码也同时显示在这上面。
3. 考虑购买嵌入式跟踪设备，比如 Absolute Software 公司的 Computrace LoJack for Laptops，尤其是当电脑里保存的信息非常重要时。这类嵌入式的设备都很不错，但是那种集成在主板上，无法通过探测硬盘频繁（比如每天）备份（数据）到可移动存储设备也是一种最好的做法。究竟选用嵌入式的设备还是物理设备，取决于对你们来说是防盗更重要还是事后追回更重要。如果丢失的物品本身的价值与它所保存的信息一样重要，那最好还是既安装预防装置，又安装追缴设备。

4. 对于那些需要带着个人身份识别信息(personally identifiable information, PII)四处奔波的行政人员来说，一定要把 PII 存储在带有生物验证措施的可移动存储设备上。另外，要加密硬盘驱动器，而不是文件夹和文件。这就是解决差旅人员忘记删除下载的 PII 的办法。

当设备失窃或遗失后，最重要的就是按照一个标准的流程操作。这就需要你们在事前先拟定这样的计划。下面这几个步骤应该是少不了的：

1. 在一些技术细节上协助当地执法部门。有些在 IT 专家看起来显而易见的事情在执法部门看来未必如此。比如，要提供尽可能易懂的技术细节供调查。像 IP 地址这些相关信息就应该尽可能详细地提供，以便警方、地方检查官以及书记员理解。
2. 大多数笔记本电脑被盗后都会被销赃。有些是在合法的网站上出售（这样的话就很难追查了），但是很多窃贼都急于转手，因而会选择到当铺典当。因此，把公司联合当地当铺的防盗计划公开是个不错的办法，这样可以让有所企图的人知道这些物品会被追踪并缴回。这也是完全对当铺经纪人有利的，因为一旦发现他/她窝藏赃物，那这些赃物会被立即缴回，分文都不用付给经纪人。小偷需要销赃的地方，如果最可靠的经销商都不愿意接手某些东西了，那他们也就不会对这些东西下手偷窃了。
3. 在公司内通过安全培训，视频和海报宣传这些内容。鼓励他们报告可疑人员。这种培训应该由德高望重的人来指导。不光要考虑到内容，还要考虑到讲授内容的这个过程。
4. 当电脑被追回之后，可以考虑公开做了些什么和谁做的。让人们明白严肃对待盗窃问题有助于防范盗窃，付出的努力得到肯定能激发持久的动力。

发生在伍斯特理工学院的这起盗窃案件，关键就是调查人员立即知道了事件的发生，因为失主在数小时内就进行了报告，而非数天之内。而且学生还在笔记本电脑里安装了跟踪软件，这让 Computrace 得以跟踪到这台笔记本并帮助追回了它。

有一点要注意的是，并不是在表格里填完信息后让司法部门走流程就完事了。作为网络安全分析师，我得解释可能的原因，那样司法人员--以至书记官和大陪审团--才能明白这起失窃案为何要归罪于这名窃贼。

虽然在信息安全防护上，正如常言所说,预防胜于治疗，但是事先准备好补救措施以防万一也不失为上策。

原文出处：http://www.searchsecurity.com.cn/showcontent_23889.htm

(作者：Neil Spellman 译者：Sean 来源：TechTarget 中国)

移动设备安全策略

在2007年Gartner公司无线与移动高层首脑会议上，分析师们描绘了一副可怕的场景来表述各公司陷入解决移动和无线安全问题的困境。按照John Girard的意思，超过三分之二的企业会经历由于移动用户不恰当地连接到不安全的服务或者下载恶意应用程序引起的安全问题。分析师John Pescatore预测说，在2007年移动恶意软件会变得司空见惯，在2009年上半年攻击会引起真正的业务中断。幸运的是，大部分这些恶意攻击利用的漏洞是可以确认并解决的。在本文中，我们会盘点一些使移动设备无线服务安全的策略。

网络犯罪：正在通过移动设备靠近你

无线PDA和智能手机已经使用了很多年，但很少有关于安全鞋漏的头条新闻爆出。Pescatore提出：不安全的移动设备已经飞到了雷达下面，因为移动设备恶意软件编写者受到了平台和操作系统多样化的限制。他说：“肯定已经存在了一些移动恶意软件，但是这些软件大部分没起作用，造成的实际破坏很小，而且也没有蔓延开来。”例如，最近McAfee调查了200个移动设备用户，发现83%的用户遇到过移动恶意程序的攻击，但是这些事件中只有五个影响超过了10万台移动设备。

然而，恶意软件的影响可能会发生变化，随着移动从业人员的增多，移动环境变得越来越统一，业务系统的连接面更广了。“现在已经到了企业开始部署安全进程、架构和控制来防御移动恶意软件的年头了”，Pescatore建议说，“大量蠕虫和病毒不是真正的威胁……移动恶意软件会更有针对性地对特定的设备，应用和业务出现。企业保护策略需要寻求新思路开发新方法”。

移动服务使用的无线接口是另一个病毒传递攻击的方向。John Girard相信存在范围很广的无线服务攻击很少，因为运营商会保证他们自己的网络安全。他说：“数字卫星和电台网络采用双向认证和强加密方式，阻碍试图窃听，跟踪通信或者解密数据和声音流的行为”。形成鲜明对比的是，Wi-Fi和蓝牙攻击频繁，这是由于遗留的漏洞未打补丁，也由于终端用户的配置不当。“智能手机Wi-Fi功能仍然不幸地是重复（那些相同的】老问题的另一个漏洞。”

逆转形势

大部分公司都很熟悉 Win32 恶意程序和无线漏洞。保护商业 PDA 和智能手机的一个有效策略是需要结合已有的最佳实践和新技术新工具。

1. 像 Win32 记事本程序一样，具备 Wi-Fi 和蓝牙接口的移动设备必须安全地配置好，利用健全的数据链路安全选项（如 WPA2-Enterprise），禁用有风险的选项（比如发现蓝牙设备）。内部无线网络中的活动可以通过最佳实践（如 802.1.X 和 WIPS）来监视和控制，它不依赖于客户端设备的类型。在从 3G 运营商漫游到公司无线局域网，到公共无线热点区域时，为了实现统一的端到端通信安全，将会需要像移动 VPN 这类新工具。在 3G 服务可用，而且比较廉价的地方，移动设备可能会为了降低风险考虑，把那里提升为热点区域（hotspot）。最终，公司应该设法给所有新移动商业应用和客户端服务器接口加上安全措施。
2. 移动设备可以配备客户端安全措施，类似于一直在 Win32 记事本上使用的安全措施，从加电验证，数据加密和备份恢复到防火墙、VPN 以及防病毒。移动操作系统目前仍然处于追赶竞争对手的发展过程中，所以经常需要额外增加专门为移动设备上运行设计安全软件。Girard 估计到 2010 年的时候，每年在所有这些移动安全工具上的花费将会超过一开始购买一台普通智能手机的成本。各公司可能想给在关键业务流程中使用的 PDA 在这方面做短期投资，所以就强烈要求在将来向供应商购买的移动设备中带上这些安全功能。然而，Pescatore 警告不要单单依赖于客户端移动设备杀毒。他说：“在绝大部分同类的 Windows 平台上，这都是不够的， 将来在同类移动设备上也是不够的。”
3. 相反，移动客户端安全措施应该辅之以服务端保护，包括在公司邮件服务器和移动通信服务器上的恶意软件清除。“企业应该关注同步服务器，无线应用网关和从 2007 年开始提供服务的外部无线网络服务提供商，关注在这些方面恶意软件内容保护的投资，”Pescatore 表示。企业还可以在服务端采取措施，比如：文件活动监视，数据库活动监视，用消息内容过滤来跟踪和控制移动设备对公司数据的使用。最后，网络网关可以使用网络访问控制（NAC）授权有选择的访问给属于员工的移动设备，或者阻止私自接入公司的移动设备访问。这些多样化的措施可以有效缓解大范围的问题，但是他们都需要在 IT 部门控制之下（至少在一定程度上）才起作用而且对移动设备用户是透明的。为减轻 IT 机构负担，一些公司可能采取从无线运营商或者第三方机构（比如 iPass）外购一些移动安全方面的任务。

结论

现如今大部分商业用途的 PDA 和智能手机都是“自带便携”型的设备。许多雇主都没办法列举出所有访问他们网络、服务器和数据的设备，能快速采取行动阻止主流移动设备恶意软件爆发的就更少了。第一次爆发可能很快就会出现，也可能几年也不出现。不管是哪一种情况，开始考虑移动设备安全策略已经成为了一种简单的常识。你可以通过对你单位全体员工已经在用的移动设备建立清单来估计问题的大小，按照商业风险采取短期行动减轻当前移动环境中的脆弱性。然后在没有把安全策略纳入长期计划前，抵制住部署移动应用和设备的诱惑。

原文出处：http://www.searchcio.com.cn/showcontent_23847.htm

(作者：Lisa Phifer　译者：Eric　来源：TechTarget 中国)

移动设备网络防御战略

不负责移动设备的管理者可以通过维护关键设备，如公司邮件服务器、移动应用网关、远程登录集中器和网络门户，来使得他们的网络可以抵御移动恶意软件。

例如，大多数企业已经在电子邮件出现在终端用户前进行了过滤，从而屏蔽掉垃圾邮件和钓鱼网站。无论反垃圾邮件措施是在企业邮件服务器还是在托管的电子邮件提供商处实施的，都会使移动设备受益。但是，一个必要的措施可能是设法确保所有的移动电子邮件都通过这些过滤器传递，可行的方法是阻止企业电子邮件发送到个人的 POP 邮箱中。

当移动设备通过应用网关或远程访问集线器（remote access concentrator）访问企业网络时，恶意程序可能被设备指纹或内容监测工具阻止。例如，设法限制通过设备标示符或支持的操作系统/浏览器类型对设备的访问。通过网络反病毒、入侵防御系统(intrusion prevention system ，IPS)或统一威胁管理（UTM）平台，转发所有通道上的流量，丢弃可疑的信息。但这些措施并非固若金汤，现有的网络防病毒系统或许能检测出 Win32 蠕虫病毒，但对这些病毒的 Windows Mobile 版本不一定同样有效。但是，它们可以帮助将网络与安全威胁隔离开来，因为这些威胁可以使用不受保护的移动设备绕过台式机或笔记本的防御体系。

一个万无一失的、能够阻止企业数据被移动恶意软件窃取的方式是：阻止敏感数据存储在移动设备上。可以考虑让移动应用程序和数据访问使用只读端口。例如，在图像（而不是文本）格式下呈现应用的内容，阻止文件和附件下载。你需要决定哪些类型的内容应该还是不应该放置到移动设备上，权衡移动设备的使用和商业风险的关系。

PDA 和智能手机安全的未来

从长远来看，多数管理者将把移动终端和基于网络的防御措施结合起来，像对待笔记本电脑和平板电脑那样对待智能手机和掌上电脑。然而，高速无线广域网连接的出现有可能会提供更多的移动安全防御措施。

例如，一些运营商已经可以为所有的移动设备提供与操作系统无关的、电子邮件和手机短信过滤服务。相较于为智能手机和笔记本安装常驻系统的反恶意软件程序，“云端”

战略或许可以提供更为简单的方法。展望未来，企业应设法使用安全的无线广域网服务，从而减少各种来自恶意软件的威胁。

原文出处：http://www.searchsecurity.com.cn/showcontent_28954.htm

（作者：Lisa Phifer　译者：Sean 来源：TechTarget 中国）

智能手机移动设备面临的安全威胁及应对策略

如今，许多公司的 IT 部门需要做这样一项工作：使工作人员能在掌上电脑（PDAs）或者智能手机这类的无线手持设备上处理商业数据。在理想的情况下，所有的这些设备都是值得信赖的，并且不受恶意软件的干扰。可现实的情况是，许多设备都处于无人管理也没有安全保障的状态，这就成为手机恶意软件感染的理想目标。

企业如何才能在这些问题泛滥前，将潜在的风险遏制在萌芽状态呢？

智能手机和掌上电脑的安全威胁日益增加

和 Win32 平台上的情况相比，手机恶意软件的数量仍然很少。迄今为止，已被发现的、专门针对移动操作系统的病毒、蠕虫和特洛伊木马不到 500 例。大多数只造成相对较小的损害，诸如：文件丢失、硬件重置或产生额外的话费。

不幸的是，长期制约恶意攻击的门槛正渐渐消失。首先，移动设备的使用人数正飞快增长。其次，新型热门商用消费级终端设备（如苹果公司的 iPhone 和 HTC 公司的 Android G1）的市场可能最终会发展成一个利润丰厚的市场，吸引到大量恶意软件开发者。

此外，现代智能手机已不再受制于狭窄的无线覆盖范围、单一化的操作系统或兆级别的存储容量。近乎无处不在的 3G 及 Wi-Fi 简化了恶意软件的无线传播，而数 G 字节的存储容量使得更多的敏感数据会被窃取。

随着用户越来越多地通过移动设备使用电子邮件和上网冲浪这些应用（这也是传统恶意软件的传播媒介），这使得恶意软件的传播变得更加可行。而短信服务（SMS）和多媒体信息服务（MMS）也成为传播恶意软件的新方式。

最后消失的一道门槛可能是：那种容易让攻击者妥协的单一的移动开发环境。在过

去，各种不同规格、封闭的开发环境常常使恶意软件无从下手。而塞班软件公司 Symbian Software Ltd. Series 60 系统则因开发环境友好，成为被攻击次数最多的移动平台。如今，Android 和 Linux 正建立起开放的系统开发平台。那些存在于 MacOS 和 Win32 环境中的恶意软件，也有可能入侵 iPhone 和 Windows 的移动开发平台。

智能手机和 PDA 安全软件

幸运的是，随着移动设备变得更加强大，移动操作系统的安全模式以及第三方的安全程序也得到了发展。移动智能手机和 PDAs 的管理者可以安装上这些现成的防御软件来检测和阻止移动恶意软件的安装和执行。

首先，可以通过检查所有移动设备的可执行文件和安装文件的数字签名。这些数字签名包括塞班（Symbian）或微软 Mobile2Market 签署的认证程序，以及 Research In Motion 公司针对黑莓的控制 APIs。通过使用像黑莓企业服务器或 Sybase 公司的 Afaria iAnywhere 这一类的移动设备管理工具来管理安装文件，可以帮助用户防范移动恶意软件的自动安装。另外，可以创建移动软件白名单和黑名单，教会用户如何避免运行未签名代码，并明白这样做的原因。

下一步，利用移动操作系统的访问控制，阻止恶意软件篡改文件和调用敏感功能。例如，塞班 9 的权限管理政策可以限制程序访问系统和/或用户的文件及网络接口，而数据锁定可以把数据划分到私人文件夹里，并对不受信任的程序不可见。配置这些访问控制策略有利于阻止间谍软件窃取数据，防止特洛伊木马留下后门。

最后，不同于笔记本电脑的是，移动手持设备没有在出厂时安装防火墙、杀毒软件或垃圾邮件过滤器。可以考虑通过安装常驻于系统的移动安全程序设备来填补这些空缺。例如，适用于一般的移动操作系统的防病毒和 SMS 垃圾邮件的程序（这些移动操作系统厂商包括 AirScanner、F-Secure、McAfee、赛门铁克、SMobile 系统、趋势科技和 Sophos 等

公司）。这些程序精于处理移动设备的威胁，如检测移动操作系统的特洛伊木马、过滤短信，阻止恶意软件入侵企业服务器。

原文出处：http://www.searchsecurity.com.cn/showcontent_28903.htm

（作者：Lisa Phifer　译者：Sean　来源：TechTarget 中国）

移动设备上的应用程序安全

想跟你的竞争对手秘密分享你的社会关系吗？有应用程序可以办得到。需要偷偷地密切监视员工或者配偶的动态吗？有应用程序可以办得到。想得到移动交易的密码吗？还是有应用程序可以办到。

这不光是开玩笑，随着移动应用程序下载网站的增多，现在 iPhone 和 BlackBerry 用户可以选择的企业手持设备第三方应用程序数量空前巨大。Jupiter Research 公司的最近一项研究表明，一直到 2014 年，移动应用程序每年的下载数量将达到 200 亿次。而由于想要偷窃个人网络信息、个人资料的移动应用程序大量涌现，网络安全工作人员所面临的挑战也越来越大。

随着移动设备以及第三方应用软件的增多，企业开始面临一些安全风险，其中最引人注目的可能就是这些设备和软件有可能会变成“恶意软件”以及“非法获得隐私信息软件”的传播平台。由于 IT 厂商内部集成和支持第三方应用程序的压力日益增加，他们对相关入侵威胁载体的防护能力会受到诸多限制。

美国马萨诸塞州 Northborough 市 J. Gold Associates LLC 公司的总经理兼首席分析师 Jack E. Gold 说，“随着这些移动设备的增加，肯定会有人想做一些不道德的事情：感染设备、破解网络、偷窃数据、传播恶意软件，等等”。

移动设备、应用程序的安全：政策与技术

许多第三方移动应用程序下载能够很快破解企业的网络安全，如苹果公司现在提供的一些应用程序，能够直接在公司的应用程序中对数据进行操作，SAP、Oracle 以及其他的销售自动化工具也有类似功能。环境的快速变化需要你在制定政策以及技术方面都必须警惕。

Gold 指出，单靠政策的话实施起来会比较困难，除非有一个自动化的政策管理系统，比如 Sybase 公司的 Unwired Platform 或者 Symantec 公司的 Mobile Management 等，它们可以主动监视每个电话上面的政策。然而，这些产品价格昂贵，而且配置起来比较复杂。

Gold 说，“一个公司可以很轻松的说：这些设备就是你以后将会使用的设备，在这个设备上也只有这些应用程序。然而，如果真这样做的话，最终用户的选择将会受到限制，工作效率也会下降。世界上没有任何绝对的事情，而且因为个人企业自身存在其局限性，肯定需要有更多的选择余地。而如果你所在公司的 CEO 过来跟你说：‘我要这个’，那么你需要做的工作要么是把这个应用程序放入设备中去，要么你另谋高就。所以说，这里面还存在着一个需要平衡各方权益的问题。”

为了更好的控制无线设备，企业往往选择采用他们自己 IT 部门所配置的智能手机。虽然这对于那些认为员工使用移动设备具有高风险的企业来说无疑是一个费时又费钱的工作，但这会让执行安装和使用第三方应用程序的政策变得更加简单。对移动设备进行“安全强化”跟有线通信类似，应该关闭、禁止或者卸载那些不必要的服务或者那些有严重威胁的服务。

一些规模更大的企业，如 Kraft 食品公司，他们却在使用更多的智能手机和移动设备。Kraft 公司 GIS 部门的高级副总裁 Mark Dajani 了解到虽然公司有相关的 IT 政策规定，但是员工使用智能手机还是比过去增加了，所以他的部门不仅给关键员工提供 iPhone 手机，而且并不反对使用私人设备。

Dajani 主动提供室内应用程序，包括 email、日历以及联系（contact），而且让用户直接连接 Kraft 的 Microsoft Exchange 服务器。这一做法不仅使得员工可以获取公司提供的信息，而且还提供了企业级的安全。为了访问公司财产，用户在接触网络资源之前必须通过认证。Kraft 没有浪费资源试图把个人移动设备排除在外，他选择了集中力量支持而不是禁止。

原文出处：http://www.searchsecurity.com.cn/showcontent_31778.htm

（作者：Sandra Kay Miller　译者：Sean 来源：TechTarget 中国）

如何锁定移动设备 确保企业数据安全

尽管企业和厂商都对通过 Email 或网络造成的数据泄露相当重视，但事实是，敏感的公司数据更有可能通过丢失的手提电脑、CD 盘或 USB 盘落入他人手中。以下就是几个真实发生的实例：

1. 2006 年五月份，美国退伍军人事务部门透露，一台包括两千六百万名退伍军人个人信息的手提电脑失踪。信息实际上是保存在一个移动硬盘上。
2. 2007 年十月份，英国税务海关总署丢失两张 CD 盘，包括两千五百万名英国公民的财务记录。
3. 2006 年二月份，一名德勤会计公司（Deloitte & Touche）的员工将一张包括 9290 名 McAfee 公司员工信息的 CD 盘遗忘在一家航空公司的座位后面。
4. 2007 年，报告显示，包括敏感军方信息的 USB 盘在阿富汗的街头售卖。

对手提电脑可以采用全磁盘加密（full-disk encryption），但是，可移动设备却带来更多的挑战。移动办公的员工在出差时，有合法的需求需要使用这样的设备来传输数据，甚至敏感数据。以前曾有专用的硬件用于此用途，但价格下跌幅度太大，现在甚至在一个会展上，容量上兆的 U 盘都免费赠送，而且，如今也很难发现一台手提电脑不跟配 CD 或者 DVD 光驱。

虽然仍然有些公司会让技术人员在客户端机器上锁定 USB 端口，限定 CD 为只读，但是，大部分的企业还是依靠软件的解决方式，来管理这些潜在的数据泄露问题。让我们来看一下几个软件解决方案：

1. 在 Windows XP 和 Vista，可以利用组策略对象(GPO)限制设备的安装。Vista 提供的策略比 XP 更加细化，但是，已经由用户安装好的设备可能仍然还是可用，这要看组策略对象是怎么配置的。这个是免费提供的，但其灵活性可能不如其他解决方案，还有提供的安全性也有限。
2. 许多第三方的软件工具能够限制移动存储的使用，包括 CD-ROM 和 USB 设备。策略可以非常细粒度，只有公司批准的设备才能访问，连接数码相机和音乐播放器只允许只读，而同时仍然可以阻止来自外部的数据传输。多数工具支持基于角色和系统的策略，允许对不同的用户和电脑组规定不同的限制（例如，所有的台式电脑完全禁用写入访问，但高层的手提可以启用）。

3. 阻止或审计对移动存储访问的第三方软件。策略允许访问，但同时保留一份这些文件的安全备份，然后，在下一次手提电脑连接到公司网络时，发送到管理服务器。这样，管理员就可以审阅活动，包括文件的内容，以判断是否符合公司政策。
4. 对移动存储进行可选或必选数据加密的加密软件。用户可以在公司和组密钥或者选择带密码的自身解密归档进行选择（视策略而定），来传送给不使用同一加密软件的合作伙伴。有的工具可以基于用户、组、系统或者存储设备实行策略。
5. 符合集中策略的专用 USB 设备。这恐怕是最贵的选择，不提供任何优于软件解决方案的实际安全好处。
6. 具有终端保护的数据丢失防护（DLP）产品。这些工具能够基于被检测的内容应用动态的策略。例如，可以对一个包括信用卡号码的文件加以限制，但是不包括敏感内容的 PPT 就可以进行传送。最好的工具使用深层内容分析，不仅仅保护易于识别的内容，例如信用卡号码、银行帐号，而且还保护半结构化数据，如被保护文件的一部分。有些工具包括加密，或者使用合作方的加密。DLP 是具灵活性的选择方案，所有工具都将最终包括基于内容的能力。不过，他们定义策略更为复杂，成熟程度的差异不均。

企业有多种方案可以选择，从简单的阻止设备的使用到实时的、与动态加密相连、基于内容的策略。最适合贵公司的解决方案要视公司的具体需求、用户的接受程度、预算和现有的基础设施而定。

原文出处：http://www.searchsecurity.com.cn/showcontent_3524.htm

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