办公移动化下的
数据安全手册

办公移动化下的数据安全手册

从当年的大哥大到现在的智能手机，移动设备发生了巨大的变化，而且这种变化也正不断改变着我们的生活方式。iPhone，iPad，Android，黑莓等移动设备随处可见，移动办公也越来越流行。可是很多企业还没有良好的移动设备管理策略，导致重要的数据被泄漏，损失重大。

IT 移动化下，如何保证企业的数据安全？如何在不影响员工移动办公的情况下，控制移动设备对企业网络的访问？

新趋势需要新的策略，本技术手册将从三个方面，包括移动设备安全风险分析，保护移动数据安全的方法，以及实例讲解：如何保证移动办公用户的安全，为你提供移动应用环境中的数据安全保护建议。

移动设备安全风险分析

尽管随时随地都有人在使用移动设备，但很少有人注意到它所带来的安全风险。或许有些信息正从你的移动设备中发送出去，但你从未察觉。认识到安全风险，才能更好的实现安全。这一部分中，我们将带你一起来认识一下移动设备的安全风险。

- ❖你必须知道的移动设备安全风险
- ❖小心你的应用程序　减轻移动定位服务技术所带来的安全风险
- ❖移动设备如何管理：部署变更和安全防护

保护移动数据安全的方法

了解了移动设备安全风险后，我们该采取什么措施来保护数据？由于企业信息的价值要远远超过设备自身的价值，所以专家们建议，IT 管理者要有一套移动设备的管理计划，要能够在设备被盗时恢复信息。本部分介绍如何建立安全策略应对移动设备威胁。

- ❖建立安全策略应对移动设备威胁
- ❖创建公司移动手机策略防止移动手机恶意软件
- ❖五大移动数据保护最佳实践（上）
- ❖五大移动数据保护最佳实践（下）
- ❖企业 Android 安全：移动手机数据保护建议

实例讲解：如何保证移动办公用户的安全

在了解了移动设备安全风险，掌握了移动数据保护方法后，如何在实际环境中实施移动数据保护？本部分将以一个实际案例，为你展现移动数据保护的具体过程，帮助你在实际操作过程中作出判断。

- ❖保证移动办公用户的安全

你必须知道的移动设备安全风险

从十多年前开始 CIO 们就面临着移动设备的安全问题。首先是黑莓手机，然后是上网本之后出现的诸多智能手机，直到现在苹果（以 iPad 和 iPad2 引领了平板设备的潮流）的产品。由于这些产品已经被客户所广泛使用，所以 CIO 们除了考虑内部设备的使用，还必须关注客户用自己设备连接网络时所带来的安全风险。

那么关于移动战略 CIO 最关注的是什么？要注意哪些风险？下面就是在移动设备安全策略涉及的四个主要方面：

- **升级**：在管理智能手机、平板电脑、上网本及其他设备时，最大的挑战就是及时的升级维护。当设备厂商、操作系统厂商和运营商发布各自新功能的同时，新的安全威胁也在每天涌现。对此已经存在一些工具比如微软的 System Center Configuration Manager 和 Mobile Device Manager，它们可用在一定程度上缓解安全风险。但是对于流行的设备诸如 iPhone、Android 和 iPad 来说就必须加倍小心了，因为这些设备没有集中式的升级方式，你只能寄希望于用户和苹果公司了。

- **供给**：你是否允许用户用自己的移动设备连接到你的网络？你是否进行了设备的标准化并统一分发给用户？不同级别的员工是否需要在设备联网时拥有不同的权限？用户是否拥有对敏感信息的访问权限（这要求能够在设备被窃或丢失时进行远程擦除）？如果设备可能落在不适当的人手里，你有什么办法清除其上的数据？如何管理设备和证书向客户的交付？对于所有这些问题，需要复杂的移动策略来给出答案。

- **合同和锁定**：如同技术领域内的任何事物一样，智能手机和移动设备总是处在变化之中 ——可能在你还没来得及调整相应策略之前，眼下最先进的设备已经落伍了。

就这一点而言，美国国内的厂商确实谈不上是你的朋友 - 他们的主要目标就是通过服务协议和合同来增加你的用户开销，这些协议或者合同所造成的厂商锁定时间可能是一年、两年甚至三年。因此，在谈判过程中一定要谨慎细致，反复拉锯是艰苦的，但是可以使你避免束手无策的窘境。要尽量避免厂商的锁定，不要让你所签署的合同完全是按照运营商的意志拟定的。

- **控制**：移动设备安全的第一道防线包括对所支持设备的梳理并确定哪些设备才能获准连入企业网络。对很多企业而言，这最终会导致一个所有权的问题：是否由企业购买

设备并分发给授权用户？是否允许用户自行购买设备并访问企业的邮件服务器和其他网络资源？一些公司用诸如黑莓企业服务器之类的产品来管理移动邮件访问，这种特定设备的选用为中型企业的设备选择提供了明确的界定。这种方式提供了强制性的策略——设备必须首先向服务器注册，否则无法访问相应资源。

（作者：Jonathan Hassell　译者：木易　来源：TechTarget 中国）

小心你的应用程序　减轻移动定位服务技术所带来的安全风险

最近有消息显示，诸如苹果 iPhone 和谷歌 Android 等许多智能手机一直在收集与位置相关的数据，Android 甚至每小时就把这些数据发送回 Google 几次。

这不仅引起了关于厂商道德和隐私的担忧，人们还担心其它敏感数据是否也在自己不知情或者没同意的情况下进行了传送。企业可以做些什么来减轻移动定位服务技术的所带来的安全风险，特别是当它涉及到智能手机应用时？这就是我们将在这篇文章中讨论的主题。

目前，还没有成熟的联邦法律可以防止移动设备上的数据（包括位置数据）被共享或者出售给商业伙伴。联邦政府或许会尝试介入并保护移动用户的隐私，但是任何法律想要对供应商如何收集来自手机和应用程序的数据产生影响还有一个漫长的过程，而且肯定不能指望它们（法律）来保证许多企业所需的安全等级。

Google 已经禁用了几个违反其许可协议的应用程序，但是关于应用程序如何使用和共享数据的详细信息的普遍缺失、以及安装时含糊不清的点击通过协议，意味着那些允许访问通讯信道的应用程序都有可能对企业的遵从规则和数据安全造成风险。

企业可以选用的一个解决方案是禁止使用定位服务。苹果、微软以及黑莓制造商 RIM 公司默认开启位置服务，但是它们都提供了关闭这些服务的选项。但位置数据使手机网络路由呼叫更快、更有效，同时员工将会发现，在失去位置服务后，许多有用的工具忽然变得不再那么有用了。收集位置数据除了会引起道德问题外，大多数用户并不太可能会因为这类信息而处于真正的风险之中。但是，如果其它信息从智能手机上被传送出去呢？

华尔街日报的研究发现，在 101 个最流行的智能手机应用程序中，有 47 个会发送位置信息给其它公司，并且有 5 个会发送年龄、性别以及其它信息。其中一个被测试的应用程序是 Pandora，它会传送位置信息给 7 个不同的公司，发送独特的手机识别码给三个公司并将人口统计数据发给两个公司。来自美国宾夕法尼亚州立大学和英特尔实验室的研究人员调查了 30 个流行的 Android 应用程序的行为，发现其中三分之二都显示出研究人员所称的敏感数据的“可疑处理（suspicious handling）”。其它的应用程序会在没有任何明确许可的情况下发送手机号或者 SIM 卡序列号。因此，Google 应用程序研发者以及它们的分支机构能够收集到的信息包括用户下载了什么应用程序，以及他们观看、阅读和购买了什么东西。

仔细阅读任何应用程序或者插件的终端用户许可协议是评估它是否适合企业使用的第一步。当得知这些应用程序能够访问用户的计算机上所有浏览历史、网站数据以及书签之后，谷歌从其 Chrome 网络商店里删除了至少两个游戏。一个博主发现了隐藏在某种应用程序终端许可协议里的一页，上面这样写到，"这个项目可以读取你访问过的每个页面。.....除了看见你的所有页面，这个项目还可以使用你的凭证（cookies）来从网站上请求数据。"且这些难以置信的宽泛权限居然是默认开启的。

即使一个终端用户许可协议看起来是可以接受的，但是企业不能盲目地信任应用程序来处理它们可以访问或者收集的信息。考虑到为了真正地减轻由于智能手机应用程序把数据发送给第三方而造成的风险，必须对可以访问企业网络的手机上所使用的任何应用程序执行一个全面的风险评估。这将使用诸如 Wireshark 或者 Ethereal 的网络协议分析工具来捕获和浏览应用程序所产生的流量。如果这样的测试显示正在发送的数据违反了安全策略，那么这个应用程序就不应该被批准。

考虑到需要连接回相应供应商服务器的程序数目，因此这类测试也应该在普通桌面应用程序上执行。虽然大多数程序会检查是否有更新需要安装，但即使是这样，也可能会捕获并发送那些不应该被企业外部共享的运行环境数据。

这种与数据丢失保护（DLP）技术相结合的流量分析，有助于检测和防止由于安装应用程序而引起的未授权使用和机密信息的传输。但是，由于企业网络周边之外的安全性始终是较弱的，所以智能手机能够访问的数据应该始终受到控制，并且智能手机也应该被视为不可信任的

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

移动设备如何管理：部署变更和安全防护

智能手机已经广泛地应用到我们日常的工作和生活中，然而有些 CIO 在考虑网络的安全管理时把这些移动设备遗忘了。而由于这种管理缺失，导致智能手机和其他移动设备成为了企业网络中最为薄弱的一个环节。

下面是移动设备管理的两个关键方面：

- 移动设备的升级（及其他变更）部署和管理
- 安全性，或者说对移动设备的全天候安全防护能力

移动设备的变更部署

如果你使用了移动设备，那么很可能是 RIM 公司的黑莓、苹果公司的 iPhone、Android 手机或者微软的 Windows mobile 手机。如果你的网络中只有一种移动设备的话，那么你足够幸运——然而，绝大多数情况下，企业需要同时通过不同的工具来管理多种设备。

RIM 公司具有多种设备的管理的丰富经验，其黑莓企业服务器（BES）可以让你通过一个控制台进行管理，而且能便捷地实现黑莓操作系统的升级并从桌面监控整个升级过程。BES 已经问世有一段时间了：事实上，当 2007 年针对夏时制做了改进之后，黑莓管理员就再也不用面对时间变更的梦魇了 – 通过 BES 服务器就能实现夏时制补丁在所有移动设备上的升级。因此，如果要管理黑莓设备，BES 是最佳选择。

对于 iPhone 用户来说，为了对设备进行软件升级必须部署 iTunes。如果你有多个 iPhone 设备，则应该考虑把 iTunes 部署到工作站上以确保所有设备的一致更新。其他手机则通过本地和远程的方式进行升级。总之，如果需要管理多种智能手机，你就要么对各类升级进行管理，要么干脆改变部署的策略。

移动设备的安全防护

谈到安全性，最基本的就是要对远程设备拥有控制权。对于黑莓手机，BES 可以帮你实现安全策略的控制。对于其他所有设备，Exchange ActiveSync Policies (EAP)是合适的选择。尽管 EAP 最初是为 Windwos Mobile 设计，但是现在已经演化成了各种智能手机的标准

控制策略——iPhone、Android 和微软的智能手机都通过这些策略实现对设备的控制。无论黑莓抑或是其他智能手机，下列安全特性都能通过 EAP 实现：

- 密码和数据安全：对你的移动设备实施较强力度的密码策略。而且，在一定时间的非活动状态下锁定设备，只有用复杂的密码（字母加数字）才能解锁。如果设备遗失，要能对其进行远程擦除。这样就可以在设备落入不法之徒手中时防止机密信息被窃取。

- 加密：绝大多数设备都有不能被禁止的强加密功能。比如，iPhone 上的 iOS4 使用了 256 位的 Advanced Encryption Standard 来进行信息编码 – 其他设备也使用类似级别的加密措施。必须确保所有设备都用强加密策略锁定，以便保护数据和机密信息。

- 应用安全性：通过 EAPs 或者 BES 服务器实现与移动设备的连接（注意，EAPs 不支持黑莓手机），你可以对应用的设置和可访问性进行控制。比如，你可以允许或者拒绝在移动设备上使用移动存储。你也可以只允许有签名的应用才能安装在移动设备上，以此来减少服务支持请求和潜在的问题。

- 移动 IT 安全策略：为移动设备定义强有力和简洁的安全策略。这可以通过和 IT 安全策略一起定义，但是如果太过复杂，那么会带来很多麻烦。

- 员工的认识：因为几乎每个员工都有移动设备，所以必须树立他们的安全意识。比如制定这样的政策，当员工丢失手机时，必须向你进行通报。

总而言之，你必须像对待工作站一样来管理移动设备，包括变更的部署、设备安全防护以及远程策略的实施。对安全策略的忽视将使移动设备成为网络中的薄弱环节，这是必须避免的情况。开始着手这方面的工作以未雨绸缪吧。

（作者：Danielle Ruest,Nelson Ruest 和 Marie-Andree Furlong 译者：木易 来源：TechTarget 中国）

建立安全策略应对移动设备威胁

在过去的十年中，我们的工作场所发生了很多变化，其中最大变化之一就是企业的大量信息可以离开办公室，并在雇员的笔记本电脑和智能电话中不断地移动。十年前，雇员很少在家中或是在路上工作，当然不会背着笔记本电脑到处跑。随着企业移动设备的激增，伴随而来的是信息遭受外部窃取和恶意访问。

更糟的是，攻击者都理解存储在移动设备中的企业信息的价值，并开始采取针对性的手段。

由于企业信息的价值要远远超过设备自身的价值，所以专家们建议，IT 管理者要有一套移动设备的管理计划，要能够在设备被盗时恢复信息。

在企业准许用户将其移动设备连接到网络，并下载机密的企业数据时，不管这种数据是内部信息或是客户的数据，我们都需要一套安全策略，最起码要规定设备应当如何加密。

建立策略

企业需要为移动设备的安全进行预算，因为在发生硬件丢失时，IT 部门需要认证工具及类似的专业软件来跟踪设备并删除其中的数据。

IT 管理者应当重视设备内部和外部的认证。许多可用的企业级移动设备平台包括了比普通设备自身内部所安装的认证更为强健的认证。相同的认证策略可用于所有不同类型的设备，并可推广到整个网络。

这种认证意味着在雇员每次访问设备时都必须输入口令。IT 管理者必须确保口令难以猜测，并且雇员不会将口令粘贴在某个明显的位置（如笔记本的电脑包上等）。

也许要求雇员在每次检查新邮件时都需要输入口令有点儿麻烦，但是这样做可以提醒雇员：你正在使用包含着机密信息的设备进行工作。

当然，企业的移动设备安全策略需要最适用的规则，要提供充分的帮助信息。IT 管理者要警告雇员不能将移动设备随意放置在饭店或酒吧的桌子上，而应当随身携带。在旅馆住宿时，如果不使用设备，要将其锁在保险箱或其它安全设备中。

要警告雇员，无论是工作用的笔记本电脑还是智能手机，都不要轻易允许他人使用。

设备被盗怎么办？

企业的移动设备安全策略还应当概述雇员丢失设备后应当采取的措施。通常，这种措施意味着与响应中心联系，或与 IT 部门或公司中的负责人联系，以便于及时关闭设备。

移动设备的安全策略还应当要求 IT 部门在笔记本电脑上安装设备保护机制，要安装能够远程擦除失窃设备数据的软件。谨记，移动设备的跟踪软件依赖于主要芯片厂商生产的芯片中所嵌入的技术。

在笔记本电脑丢失或被盗后，在该设备连接到互联网时，跟踪软件应当与包含 GPS 功能的设备芯片保持同步，从而可以跟踪并定位设备。跟踪软件还可以远程擦除所有的机密企业信息。此外，这种跟踪功能也可用于智能电话。

安全策略未必过分苛刻。通常，这种策略只需规定一些可行的关于设备使用的常识，并与特定的硬件和软件相结合，在 IT 部门的帮助下保护企业的敏感信息。

（作者：茫然　来源：TechTarget 中国）

创建公司移动手机策略防止移动手机恶意软件

问：现在，越来越多的攻击者以移动平台为攻击目标来获取利益。企业可以执行哪些最佳实践来防止企业智能手机成为攻击目标呢？

答：目前，智能手机安全还未发展，这就像 20 世纪八十年代的桌面计算机安全一样，但是智能手机可以从过去二三十年反恶意软件技术中获利。当犯罪分子认为他们可以从新的平台获利时，新的平台就成为了攻击目标。这也就给智能手机带来了巨大的风险，因为犯罪分子能够通过这个攻击向量直接从他们的恶意软件中获利。但是，目前攻击者仍然以攻击 Windows 操作系统为主。

移动手机恶意软件创作者为智能手机开发恶意软件，让智能手机给付费记账地点（premium billing location）拨打电话或发送文本信息到付费服务以获取利益；类似于 PC 上的拨号恶意软件。该恶意软件创作者会在这些付费服务中创建了一个 stake，为大量的向他们拨打电话或发送消息索取费用。但是，这个恶意软件还没有广泛传播，因为智能系统中使用的操作系统不同；Symbian 系统目前在智能手机操作系统市场上占有很大的分额，其他操作系统的应用也在增加。

有很多书写了关于智能手机安全的问题，但是可供企业使用的防止智能手机被利用的最佳实践样本却很少。最佳实践首先需要企业有一个移动手机策略（包含用户培训）：应该告知用户不要安装未知来源的应用程序或“破解”其智能手机。实际上，一般的智能手机中安装的软件都是默认被监管和控制的，因为许多智能手机只使用厂商支持的应用程序，如从 Apple AppStore 或 Android Marketplace 下载的应用程序。虽然恶意软件很难在智能手机上安装，但是和桌面系统一样，用户又很“愿意”安装恶意软件，当他们想在其他下载平台上下载程序时，如 Twlight Eclipse Preview。为了防止恶意软件被安装，用户应该安装反恶意软件应用程序来保护智能手机，正如 Mikko Hypponen 在黑帽大会 2010 中提到的那样。

防止恶意软件只是智能手机安全的一部分；企业也应该确保用户具有强密码；并且确保移动设备具有远程管理和信息擦除的功能，以确保它们得到足够的保护。

（作者：Nick Lewis　译者：曾芸芸　来源：TechTarget 中国）

五大移动数据保护最佳实践（上）

Juniper 网络公司的最近一项调查显示，40%的员工正使用自己的移动设备来处理个人或商业事务，其中 80%的人承认他们未经允许就访问了所在公司的网络。

除非企业实施控制，用来防止这些员工所持设备的损失、盗窃或是非法使用，否则任何一件诸如此类的安全事件都可能会使相当多的业务数据承受巨大风险。

保护企业移动设备数据的措施是众所周知的，包括从实施加密到擦除遗失设备上的数据。但是，与员工设备有关的业务数据必须得到相关保障，而不是依赖于 IT 采购和用户，同时还需要尊重用户对个人隐私和选择的期望。

以下介绍五个对员工移动设备和平板电脑上重要数据进行保护的最佳方法。

1. 移动设备锁

设备锁是 IT 业界的第一道防线，防止那些未经授权，对储存在员工移动设备或平板电脑上的业务数据和账户的访问。然而，员工购买的消费电子设备通常不具备足够强大的设备锁。还有，用户可能会重置复杂的密码而不方便个人设备的使用。这种业务需求可以通过一个三步骤方法得以解决。

- 实施一个程序让用户注册自己的移动设备和平板电脑，并按照最低安全要求检查它们。这样可以防止设备去进行不合标准的商业运用，而允许那些可以支持 IT 范畴内的安全政策。
- 自动配置已注册的设备以启动内部的 PIN 或密码锁，执行复杂的规则并自动锁定待机的设备。专注于那些可以减少商业风险而不会使之过于严格的规则。
- 实施无线设备配置监测以保证设置没有被改动。例如，对设备每一次试图访问一个企业账户的行为进行检查，从而阻止或修复不兼容设备。

如果员工移动设备中包含交互环境搭建（EAS）或多操作系统移动设备管理软件（MDM），那么就可以采取这些措施。目前这些软件已经由诸如 AirWatch、BoxTone、Good Technology、MobileIron、Odyssey Software、Sybase 和 Zenprise 这些公司推出。那些没有 MDM 也不想安装 MDM 的公司可以使用托管 MDM 服务。

2. 移动设备的远程数据擦除

当以前注册过的设备遗失/被盗或者它的主人离开了你的公司，远程数据擦除可以防止将来对存储在设备当中的所有业务数据和账务进行访问。然而，擦除员工的设备资料在没有明确的许可下是不应该的，且在理想情况下，不应对个人数据造成影响或者给用户带来不便。这些业务需求可以解决，方法如下：

- 作为设备可以注册的条件，员工必须被要求正式同意一些可接受的使用条款。移动设备条款还应该明确，在什么情况下可以调用远程擦除，怎样擦除才不会影响个人设备的使用和数据，以及数据备份/恢复的责任。
- 考虑使用数据加密工具来区分业务数据、账户和应用程序。例如，使用自加密（self-encrypting）企业信息应用程序能够将电子邮件、通讯录、日历及其他数据保存到一个需要认证的加密沙箱里，这个箱子能够轻易的被移除而不需要擦除整个设备。
- 实施能够远程擦除员工的设备的流程。为了防止逃避技术，在经过重复登录失败，长时间脱机使用或者移除了 SIM/USIM 卡的情况下，通过自动擦除可以完善无线命令确认机制。确保密切注意留在移动媒体设备（如 Android 设备）上的企业数据。

使用 EAS、任何 MDM，或许多供个人使用的免费或便宜的应用程序（如，苹果的 MobileMe，迈克菲 WaveSecure），可以实现基本的无线远程擦除。然而，更大的 IT 控制和可见性可以按照下面这种 MDM 的用法来实现：例如，报告哪部设备将被擦除，或者自动移除 MDM 之前已安装的企业应用程序和账户。

3. 移动定位和跟踪

在任何移动设备的使用寿命里，关于它的使用情况的大量信息可能会被记录，其中包括地理位置。持续跟踪能（On-going tracking）够帮助 IT 迅速恢复丢失的设备，或产生有关盗窃信息的漫游警报，警告 IT 可能发生的威胁。然而，员工对于隐私权的要求可能会阻碍持续的跟踪。此外，一些用户的设备可能不容易定位（例如，断开或禁用的设备）。最后，如果要追踪涉及到频繁的 SMS 信息，所需的成本可能相当大。

强调商业需求并且考虑到个人和成本的敏感性，决定是否真正需要将持续追踪应用到员工的设备上。如果是这样，你需要在可接受的使用政策中描述定位追踪的业务理念和具体做法，这在注册个人设备为商业使用时需要得到员工的同意。如果定位仅仅只是用来找回遗失的设备，那么你需要将这条陈述写入到可接受的使用政策中，并坚持使用这个有限制的做法。

按需制定的定位服务对每个主要的移动操作系统（例如，苹果的 MobileMe, Lookoutd 的 Find My Phone（安卓），微软的 My Phone，和黑莓的 Wheres My Phone）均可免费使用。但在这里，通过使用移动设备管理器来实施这一做法能够得到更集中的可视性和控制效果。

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

五大移动数据保护最佳实践（下）

在上一部分文章《五大移动数据保护最佳实践（上）》中，我们介绍了三个对员工移动设备和平板电脑上重要数据进行保护的最佳方法，本文我们将继续介绍两个数据保护方法：移动设备的存储数据加密和移动活动监测和审计。

4. 移动设备的存储数据加密

在一些情况下，设备锁加上远程擦除就足以减轻用于有限业务的个人设备的风险了。如果移动设备被用于检查无毒的电子邮件且不保存附件，或者只是一台用以进行远程桌面访问的平板电脑，那么它不需要储存那些永久保护的业务数据。然而，在处理敏感信息或者需要更多的功能时，员工还需要对被存储的数据进行加密。不幸的是，一些消费设备并不支持全设备加密。为了解决这一业务需求，可以采取以下步骤：

- 扩展上述注册流程来检查依托于存储数据加密需求的个人移动设备，在扩展中要使用工作人员已认证的身份来确定移动数据的需求和风险。如果必须加密但设备却不支持，那么需要为员工提供适合设备的指导，条件允许的话，甚至可以提供一个有 IT 安全保障的公司设备。

- 自动配置已注册的设备，从而在任何可能的地方都能支持全设备加密或者可去掉的媒体加密方式。凡是需要需求和风险允许的地方，都可以配置个人加密应用程序来提供另一层保护，从而使公司的数据和个人的数据分隔开。最后，还可以配置设备的设置和应用程序来最小化存储在设备中的数据量。

- 使用无线设备配置的监测来确保用户遵守了所有的数据加密政策。此外，要小心关注设备显示出的有被干扰的迹象（即，获得了 Android 设备的 Root 权限，或破解了 iPhone 手机），因为这些可能潜藏着木马，从而访问和传播用其他方式加密的数据并发送给远程攻击者。

为了实现第一步，需要将你的注册过程同公司的目录、现有身份认证登录，以及使用群组隶属关系等整合起来，从而确定业务的需求和风险。第二步，你需要配置安全的移动应用程序，如 Good for Enterprise 和 NitroDesk TouchDown，或者替换门户网站和远程桌面访问，这些措施可以用来减少某些员工的设备存储，他们其实并不需要对业务数据进行离线或分离访问。

5. 移动活动监测和审计

请注意，不断的监测对这些最优做法而言是很重要的，单单配置一个员工设备就希望业务数据可以长期安全是不现实的。即使 IT 可能不会选择或拥有员工移动设备，公司仍然需要监测和审计业务数据和活动，以确保它们在整个生命周期内都一直符合规定。然而，这必须通过无线方式来实现，从而不会对个人使用产生干扰。

- 从监测未经 IT 允许而用于商业场合的员工设备的工作环境开始，网络访问控制、设备指纹识别工具和无线/有线网络 IPS 等操作，都是帮助 IT 部门发现移动设备或平板电脑的理想工具。这些工具的有些监测机制甚至可以防止未知设备接入企业。

- 其次，记录包含已注册移动设备的每一个商业系统的交互操作，包括电子邮件/联系方式/日历的同步、网络会议、虚拟专用网（VPN）连接、在线配置更新和 MDM 应用程序安装。这些记录对日常报告和审计来说是很重要的，因此应该在设备被擦除或取消注册后长期保留。理想情况下，设备应该以某种可以防止被诈骗或克隆的方式来进行身份识别，比如说设备可以使用 SCEP 来进行授权。

- 最后，为每个注册的员工设备定期执行符合规定的检查。至少应该在正常交互操作中进行检查（例如，在每次进行电子邮件同步时，使用 EAS 来验证设置）。不过，MDM 产品通常提供了更加丰富的移动设备审计和报告功能，比如在某些情况下所进行的预定和按需设备的设置检索以及 IT 指定策略的自动对比等操作。

通过实施这五项基本移动设备数据保护最优措施，许多公司都可以接纳个人移动设备的商业化使用趋势。公司需要把注意力集中在业务数据上，并且制定出所需的最低控制，从而保障这些数据的安全。例如，很少有用户会同意白名单措施，这样会阻止他们安装个人应用程序；然而，许多用户会接受，甚至欢迎——对被盗的个人设备进行擦除的 IT 帮助。为了实现接受度最大化并避开陷阱，你需要确定一个测试组，并按照安全策略和控制对它进行初始设置，还要在公司全范围推广之前进行任何有必要的改进。

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

企业 Android 安全：移动手机数据保护建议

对消费者而言，智能手机的性能和价格要远比它的安全性重要得多。不过，对一家企业来说，手机上的操作系统和运行软件的安全性就显得至关重要了。因此，谷歌发行的第七款也是目前最新版的 Linux 手机操作系统 Android 2.2，致力于减轻企业安全管理人员对手机操作系统安全性的忧虑。这些企业安全管理人员可不希望别人接触到他们的企业资料。在本文中，我们将探讨一下 Android 操作系统在安全方面的优势和劣势，并提出一些对 Android 手机进行数据保护的指导方针。

首先，微软的 Exchange 管理员能够在设备之间执行密码政策。他们可以远程将手机恢复为出厂时的默认设置，以防手机在丢失或被盗时发生数据泄露。然而，一些没必要的手机性能（如，照相和蓝牙），却为手机增加了数据泄露的风险，无法远程禁用这些功能。

对某些企业来说，还存在规则遵从的问题。如果要使电脑上 Outlook 联系信息以及其他信息与 Android 手机进行同步，首先就要求用户和谷歌的云服务同步。目前打开一件设备，有数字 PIN 和字母数字混合密码两种选择。但是，这些密码保护措施的锁定期短暂，并且执行不力，使用起来让人们很反感。

目前，正式的数据加密措施还没有研制出来。iPhone 在芯片集上内置了加密技术，Android 手机则依赖 javax.crypto 库。Android 手机的做法无形中为自己增加了一项风险：必须确保研发人员能够正确的使用 javax.crypto 库。传闻说，iPhone 和黑莓手机的加密技术可以被破解，所以若 Android 想成功打入企业手机市场，则必须在手机安全性能上比对手做得更好。

然而，智能手机能够下载应用程序，使得它成了网络罪犯的理想攻击目标，也使得在企业网络内使用智能手机存在潜在危险。Android 手机依靠自身的 Linux 操作系统，加强了应用程序和系统之间在处理级别上的安全性，可以预防恶意应用程序造成系统范围的破坏。 不过人们发现，Android 的应用程序存在着可能导致用户私人信息外泄的漏洞。这些信息，包括位置数据，可以被发送至远程服务器，而用户对发送过程却毫不知晓，不知道发送出了什么信息，也不知道将发往何处。

上述情形是可能的，因为一项应用程序在安装时可以被授予或取消某些“功能”，就像访问权限一样，可以对设置加以限制，允许一些特定的程序可以访问或使用。然而，却没有办法

阻止程序误用它的功能。合法的应用程序也可能采用一些恶意的程序所使用的功能，这也使得用户对潜在风险作出评估变得困难。

这一点与苹果公司所采用的防护措施是截然不同的。尽管所有的程序都被看作是平等的，并可以访问许多资源，但苹果在默认情况下将其手机设置成可以对所用的应用程序进行检测和批准，借此对它们进行监管。至于检测是如何进行的尚不清楚，而且检测还需要人对其进行筛选，所以这一措施似乎还是有一定效果的。此外，手机的操作系统只允许应用程序执行在安装时所列出的功能，而这些功能都是手机操作系统需要运行的。

但对企业而言，他们需要知道一项应用程序在获得某项功能的授权后是如何执行的。谷歌回应了外界对其 Android 应用程序监管不力的指责（只是禁用了几款违反许可证协议的应用程序）。在第三方给出其应用程序的规格数据表（详细的介绍数据是如何被使用、以及被谁使用）之前，企业的规则遵从和数据安全人员对这些程序总会心存戒备。

希望使用装有 Android 系统设备的企业不太可能对其整体的移动设备策略做出大的调整。当前，没有哪个手机平台是绝对安全的，因此可以接受的手机使用政策是要求那些使用企业手机的用户遵守以下规则：只能安装获得企业 IT 部门认可的应用程序，避免打开未知文件、电子邮件、短信和即时信息。（假如是那些储存了企业数据的私人手机呢，情形就进入了管理的灰色地带。对那些技术上不属于企业的设备而言，执行此项政策是比较困难的。）

就像对待所有操作系统那样，管理员需要时时关注供应商提出的警示，与安全措施的发展保持一致，还需要安装一款为手机设计的反病毒软件包；McAfee 公司为 Android 提供的 VirusScan Mobile 对当前用户来说是免费的，Symantec 公司的诺顿 Smartphone Security 也是免费的，该软件提供了防盗和危险保护功能。

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

保证移动办公用户的安全

在跟上员工的移动办公步伐上，Kenneth Johnston 并不是一个人在战斗，Johnston 是担保银行（guaranty bank）信息系统的副总裁兼 CIO。对员工而言，扩展银行现有电子邮件在移动设备上的加密功能，是一个痛苦和耗时的过程。

Johnston 说：“我们的移动办公人员和客户设法避开身份验证过程，但失败了。实际上，加密电子邮件非但没有增加安全保护，反而加深了我们对数据泄漏的恐惧。”

于是 Johnston 转向 Proofpoint 移动加密技术，以帮助银行员工和他的银行商业客户扩展电子邮件加密功能。Proofpoint 允许用户以一个移动应用程序或者 Web 访问的形式使用其电子邮件加密服务。

位于美国密苏里州斯 Springfield 的担保银行部署了一个有效的 Proofpoint 企业套件，用以防止非认证的电子邮件收发访问。Johnston 说，移动应用程序是一个企业套件的自然延伸，为用户提供了一个熟悉的使用体验。现在，员工和客户可以快速验证，并直接在他们的设备上打开消息。

由于移动办公越来越普遍，安全厂商适时采用了新的移动设备加密安全手段，如智能手机加密。在三月份，Proofpoint 推出了新的移动应用，使移动用户可以轻松对加密信息进行解密，并支持在电子邮件文档中进行搜索。对安全厂商来说，使 IT 移动管理更容易是一种日益增长的趋势。

Ogren 集团的创始人兼首席分析师 Eric Ogren 表示，在移动设备上的扩展认证和加密已逐渐成熟。早在 20 世纪 90 年代，RSA 就在 Palm Treo 上支持 SecurID。其他新近加入的厂商包括 Overland Park,堪萨斯州的 PhoneFactor，它们提供了基于手机的无令牌双重认证系统。Ogren 表示，对不断增加移动办公设备的公司而言，延伸到智能手机和平板电脑上的安全产品是一个更有吸引力的选择。

Ogren 说：“公司最大问题之一就是在移动设备、笔记本电脑、台式机等所有设备上取得认证。将密钥嵌入到设备以便最终用户可以查看加密电子邮件是非常有效的。”

其它安全厂商也加入了战斗。旧金山的移动安全厂商 Lookout 销售在 Android，黑莓和 Windows Mobile 设备上的移动应用软件，它可以检测移动恶意软件并分析应用程序是否在

执行一个隐蔽的入侵。和其他的移动设备平台一样，Lookout 执行安全备份，这可以定位失踪的设备和执行远端清除功能。包括赛门铁克，McAfee 和趋势科技这些主要的安全厂商也提供类似的功能。

总部位于洛杉矶的 Wedbush 安全公司的副总裁和 IT 主管 Mattias Tornyi 表示，他的公司专注于针对周边设备的攻击已经很久了。但他承认，周边设备的定义不再是泾渭分明的，SSL VPN 功能是必备的。虽然使用 BlackBerry 的服务可以使公司安全地进行管理，许多经纪公司的在外场办公的员工都在使用 BlackBerry 设备，但越来越多的人转向了苹果 iPhone 和 Android 设备。我们的目标是能够安全地将帐户信息迁移到 iPad 和 iPhone 上。

Tornyi 说：“我们现在只处理随时，随地地访问这个概念。我们在保护所有的一次性令牌，我们也有正在使用的高性能的防火墙和‘入侵防御系统’。这将是一个缓慢的过程。”

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