

Carnegie Mellon
CyLab
CONFIDENCE FOR A NETWORKED WORLD



McAfee
迈克菲

移动和安全

缤纷机遇，艰巨挑战

移动和安全

缤纷机遇，艰巨挑战



目录

简介	3
二十一世纪计算的移动性和 IT 消费化	4
二十一世纪计算技术移动性安全隐患	8
安全策略与移动现实	11
基于位置的技术可提高移动安全性	17
针对企业和消费者的建议	18
总结	20

简介

Todd Gebhart, 迈克菲执行副总裁兼个人用户、小型企业和移动安全事业部总经理

数十年前，在信息时代尚未来临之前，大型机象征着计算能力，人们只能在连环漫画和科幻小说中寻觅未来通信的踪影。还记得连环漫画中那个对着双向无线电手表发号施令、勇敢无畏的侦探 Dick Tracy 吗？漫画中的未来早已到来，如今，我们不断发展进步，进入了充满机遇和挑战的新时代。

移动技术正在改变我们的个人、职业和政治生活的方方面面。请思考下面这位行业领军人物的观点。在 D8 会议上，苹果公司 (Apple) 首席执行官 Steve Jobs 说：“只有极少数人需要传统电脑的时代即将到来。正如我们过去处于农业时代时，所有的车辆都是卡车，因为农田作业只需要卡车。” Jobs 将 PC 比作卡车，说明虽然 PC 依然存在，“但将来需要它们的人会越来越少。”¹

经过长期的发展，许多从业人员将使用移动设备来完成以前在桌面上完成的大部分工作。

为完成本次报告，迈克菲与卡内基梅隆大学联合调查了移动安全的当前状态，指出了一些所有企业和消费者都应当思考的常见问题并提供了若干解决建议。

迈克菲移动和安全调查结果表明了以下几个主要趋势：

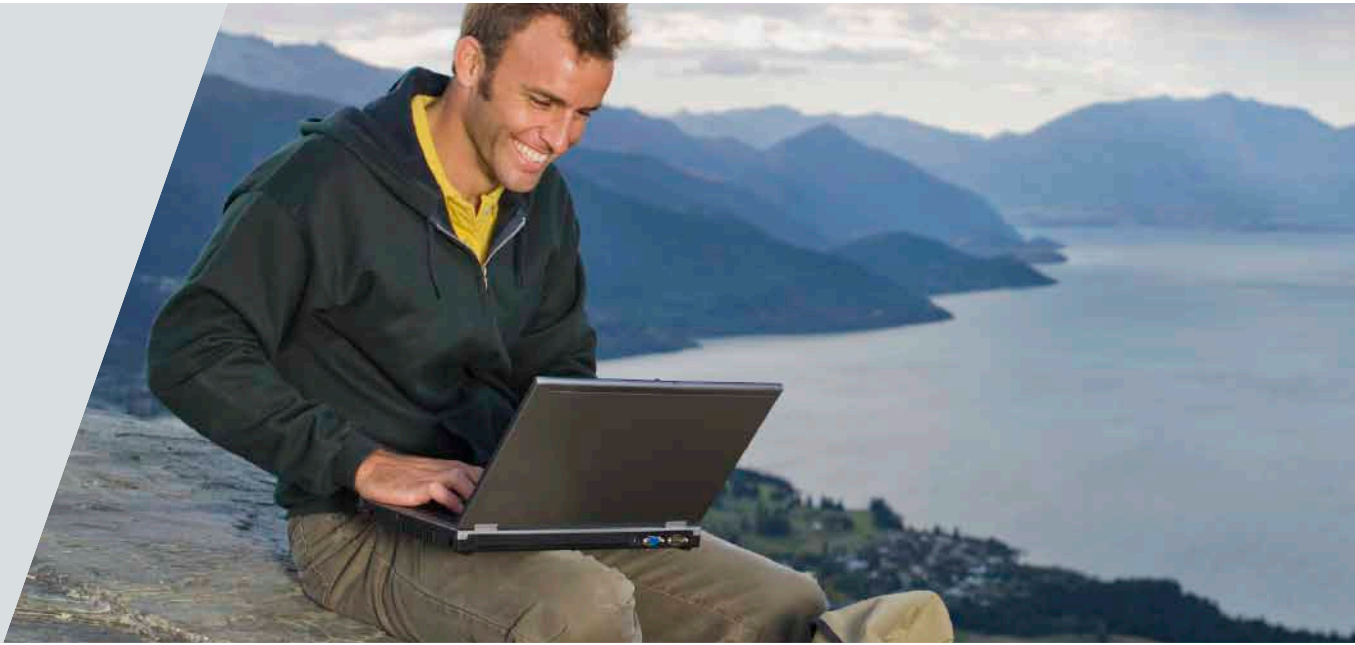
- 对移动设备的依赖性已经突显并且迅速增长；新兴移动环境越来越丰富多样且自由发展
- IT 产品日益消费化，这一点从 63% 的网络设备同样适用于个人活动便可得到证实

- 移动计算环境的策略与现实之间严重脱节；IT 总监和用户均表示不满
- 消费者和 IT 专业人士将移动设备的丢失和被盗窃视为威胁移动计算环境的最大安全问题
- 虽然人们承认必须降低移动安全风险和威胁，但是危险行为和安全状态不佳的状况仍随处可见

从银行到咖啡店再到书店，都提供移动服务，消费者在这些场所都能使用移动设备。

移动对于二十一世纪计算的本质产生了重大影响。提供了许多令人眼花缭乱的机遇，同时也带来了一些关于安全和隐私问题的艰巨挑战。那么有哪些挑战呢？这些挑战在全球的企业中又如何显现呢？

企业能否应对这些挑战，并从伴随移动计算时代而来的许多机遇中获益？它又将在哪里结束？无论在哪里结束，经历的变革都必定意义深远。



二十一世纪计算的移动性和 IT 消费化

桌面计算机的出现标志着信息时代的到来。在信息时代早期，“Windows”和“Apple”这些名词演变为全球知名的品牌名称，从而推动了一种全新的工作娱乐方式的形成。很快，整个世界都发生了变化，逐渐出现了局域网 (LAN)，然后是万维网、笔记本电脑，随后迅速发展到 WiFi 热点、智能手机、云和平板电脑。

“计算技术的最新发展助推了移动计算设备的速度和存储能力的大幅提高，” CyLab 研究人员 Collin Jackson 表示，“这些发展极大提升了我们的工作效率以及企业和个人的效率。但是，与始终位于办公室的设备相比，移动设备更容易丢失、被盗或者在无人监管的情况下被冒用。”

实际上，在美联社公布的“对人类生活影响最大的 50 件事物”榜单中，有 21 种事物与技术有关，并且与移动性息息相关：“应用程序、博客、黑莓、数码相机、手机、连接、在线约会、数码摄像机、Facebook、Google、GPS、信息泛滥、iPod、Netflix、性短信、短信、平板电视显示屏、Twitter、Wii、Wikipedia 和 YouTube。”²

回顾一下最近的一些商业新闻报道。皮尤研究中心的互联网及美国生活项目调查发现，在过去的一年中，美国人对手机非语音程序的使用“显著增加”，越来越多的人将手机用作照相机和录像机以及用于收发电子邮件、连接互联网和玩游戏。³

除了使用方式的变化外，这些设备的计算能力也发生了巨大的变化。麻省理工学院和德克萨斯高级计算中心的研究人员最近创建了一款 Android 应用程序，可以模拟强大的 Ranger 超级计算机并将其移植到手机上。⁴

Apple 公司首席运营官指出，Fortune 100（财富 100 强）企业中有 65% 的企业已经在部署 iPad 或实验项目，许多分析公司均预测在 2011 年企业中的平板设备数量将激增

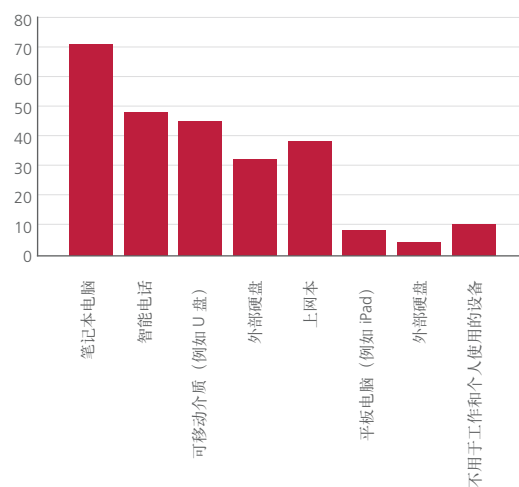
这种移动计算的迁移不只改变了用户的个人生活，也改变了他们的工作方式。越来越多的用户发现他们的企业跟不上不断变化的移动技术的步伐。Apple iPhone、Droid、Apple iPad 及其他移动平台不断涌入世界各地的企业。这种状况并非突然形成的，但是这些设备已经缓慢蔓延到了工作场所，并且大有取代之势。Apple 公司首席运营官指出，Fortune 100（财富 100 强）企业中有 65% 的企业已经在部署 iPad 或实验项目，许多分析公司均预测在 2011 年企业中的平板设备数量将激增。

CyLab 研究人员 Nicolas Christin 对单击式欺诈（某家犯罪企业成功利用网上银行和手机计算方面的漏洞进行欺诈）进行了研究。Christin 认为，移动设备带来的便利性以及销售人员可从任何位置访问公司数据的能力，改变了企业信息处理方式。

“这种转变带来了安全隐患，” Christin 说，“特别是，大规模人群出于职业和个人目的而使用笔记本电脑，而这可能会引发安全问题。攻击者能够轻松定位可移动介质以绕过防火墙等网络防御措施，例如 Stuxnet 威胁以及其他复杂的恶意软件威胁。”

IT 消费化围绕的是工作效率，但提高工作效率就不能不关注成本。很多情况下，企业看到了工作场所中这些消费设备的好处，但依然密切关注保护企业机密数据。在迈克菲以前执行的调查中，半数以上的受访者一致认为 IT 消费化增加了安全隐患，近一半（45%）受访者感到管理企业网络内部的用户设备及相关技术“至关重要”。

用于工作和个人用途的移动设备

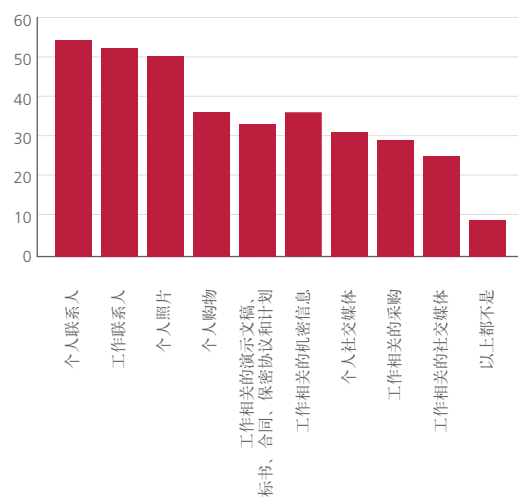




Gartner 调查报告“预测：2008-2014 年全球移动应用程序商店”（2011 年 1 月 26 日）指出，2011 年将下载 1770 万套移动应用程序（比 2010 年增加一倍），同时预计应用程序商店的收入将超过 150 亿美元。⁵

对移动设备的依赖性已经突显并且迅速增长；新兴移动环境越来越丰富多样且自由发展。

移动设备上使用的信息和应用程序的类型



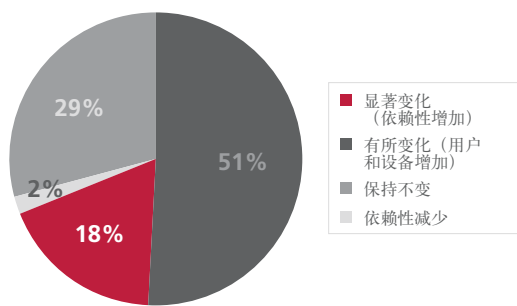
许多企业已经严重依赖于使用移动设备，近半数企业表示“非常依赖”。

至少近半数受访企业非常依赖移动设备，其中有 31% 的企业表示“非常依赖”，18% 的企业表示“极其依赖”。近 7/10 的企业今年比去年更加依赖移动设备。超过半数 (51%) 企业表示情况有所改变，同时有 18% 的企业表示状况发生了“巨大变化”。



“无论在发达国家还是新兴经济体，移动设备都将继续高速蔓延”
Adrian Perrig, CyLab 技术总监

对移动设备 (不包括笔记本电脑) 的依赖性



“无论在发达国家还是新兴经济体，移动设备都将继续高速蔓延，” CyLab 技术总监 Adrian Perrig 表示，“配有高速处理器、高分辨率触摸屏、位置信息服务和随时随地连接功能的智能手机，将提供全新的应用程序和服务。在我们的日常生活中，已经可以看到人与人以及服务之间交互方式的转变。随着智能汽车和智能住宅等新服务的推出，这些转变很可能继续加速进行。不幸的是，这些新环境也带来了新的风险和漏洞，因此我们需要随着这些技术的演进而不断应对新挑战。”

将笔记本电脑视为主要工作计算机的受访者比例 (45%) 与将桌面机视为主要工作计算机的受访者比例 (47%) 基本相同。在七个国家/地区中，人们更偏向于将笔记本电脑视为其主要工作计算机。在印度，仅有 13% 的受访者表示他们的主要工作计算机是桌面机，而有 57% 的受访者表示是笔记本电脑，16% 的受访者表示是智能手机。英国有 64% 的受访者将笔记本电脑作为其主要计算机，是比例最高的国家。在以下某些行业中，还有更多人认可将笔记本电脑作为主要工作计算机：商业和专业服务 (55%)、电子产品 (51%)、能源和公共事业 (49%) 以及高科技和电信业 (53%)。

二十一世纪计算技术移动性的安全隐患

但是，二十一世纪计算技术移动性的安全隐患有哪些呢？这是一个备受关注的问题，并且也有充分的理由受到关注。

McAfee® Labs™ 在其 2011 年威胁预测报告中表示：“2011 年，针对移动设备（包括 iPhone、Android 设备等）的攻击将升级，因为犯罪分子不断寻找漏洞进入‘脆弱的移动通信基础设施’以访问通常不加密的业务和企业通信。随着移动设备在企业环境中的日益普及，商业机密和其他重要信息外泄的机会也相应增多，迈克菲认为网络犯罪分子将不断寻找漏洞。”

针对移动设备的相关风险纷繁复杂。造成这种状况的根本原因在于，移动设备中保存了有关用户及其所在公司的大量敏感信息。

以智能手机的联系人列表为例。联系人列表通常包含与企业具有业务往来的相关人员的重要敏感信息，包括当前客户、潜在客户、关键供应商、有影响力的分析师和记者等。还包括有关用户个人生活的重要敏感信息，这些信息可能被利用进行社交工程攻击，用来猜测密码及访问企业网络。此类信息可通过多种方式获得：盗取设备、捡拾丢失的设备、安装隐藏了恶意软件的看似无害的应用程序，甚至采用某些意想不到的偶然的方式。

2011 年，针对移动设备（包括 iPhone、Android 设备等）的攻击将升级，因为犯罪分子不断寻找漏洞进入“脆弱的移动通信基础设施”以访问通常不加密的业务和企业通信。

当然，联系人列表并非获取重要情报和敏感信息的唯一来源。其他信息源包括智能手机和笔记本电脑上存储的通话记录、日历、短信和电子邮件通信。翻看这些数据会泄漏机密并暴露弱点。如果附在电子邮件中的电子表格、商业计划和标书等文档落入不法分子手中，后果将不堪设想；将移动设备遗忘在酒店大堂（即便后来将其寻回也于事无补）等常见的疏忽都可能导致安全隐患。

智能手机和笔记本电脑还可能含有拍摄和录音功能。智能手机的摄像头是许多企业严禁访客携带手机进入某些业务敏感区域的原因之一。其目的在于降低业内间谍和其他恶意活动的风险。但是，如果智能手机或笔记本电脑的摄像头被远程激活并危害个人或企业，怎么办？如果远程攻击者将智能手机或笔记本电脑在不易察觉的情况下作为录音机使用，然后带入企业核心机密区域，怎么办？如果智能手机上的照片、视频和音频文件在未经用户许可或同意的情况下被远程访问，或者由于在行业会议期间不慎遗落在会议室中而落入不法分子手中，怎么办？

这些情节不仅出自 Ian Fleming 笔下的詹姆斯·邦德系列小说，更是来自当今移动计算环境的真实场景。但移动设备的相关风险不仅限于功能强大的笔记本电脑和功能完备的智能手机。USB 记忆棒或外部硬盘等可移动介质也隐藏着巨大的风险。



来看一下维基解密事件。这件轰动全球的新闻报道引发了关于 U 盘的担忧。在美国政府机密文件泄漏后，五角大楼禁止在军用机密计算机上使用 CD、DVD、U 盘及其他可移动介质。讽刺的是，在为寻求安全性和易用性之间的平衡而不断斗争的艰难过程中，以前曾经公布过有关此类可移动介质的禁令，当时是为了阻止蠕虫攻击数万台计算机。但是这条禁令已于 2010 年 2 月取消。正是在取消最初禁令之后的几个月中发生了文件泄漏。⁶

利用移动计算技术作为潜在攻击“武器”的行为似乎永无休止。甚至 USB 连接线也被成功用作攻击手段。乔治梅森大学的两名研究人员发现了一种通过常用 USB 连接线来攻击笔记本电脑和智能手机的方法。Angelos Stavrou（计算机科学系助教）和 Zhaohui Wang（学生）编写了能够更改 USB 驱动程序功能的软件，以便他们能够在有人为智能手机充电或在智能手机和计算机之间同步数据时发动秘密攻击。⁷

两党政策中心在 2010 年开展的大规模模拟网络攻击表明，政权人士也开始产生这种安全忧虑。模拟网络攻击设想攻击在一天内迅速蔓延，导致全国 2000 万部智能手机无法使用。这次模拟攻击基于数月前通过广受欢迎的“三月疯狂”篮球锦标赛应用程序而悄悄植入手机中的一种恶意软件，它扰乱了数百万部智能手机的移动服务。而后模拟攻击逐步升级，最终关闭电子能源交易平台并导致东海岸电网瘫痪。⁸

在美国政府机密文件泄漏后，五角大楼禁止在军用机密计算机上使用 CD、DVD、U 盘及其他可移动介质。

95% 的企业已经制定了移动设备策略。但是，只有不到 1/3 的员工非常了解自己公司的移动安全策略。



安全策略与移动现实

移动计算环境中的策略与现实之间严重脱节，策略认知和策略遵守之间也严重脱节。IT 总监和用户均对现状表示不满。

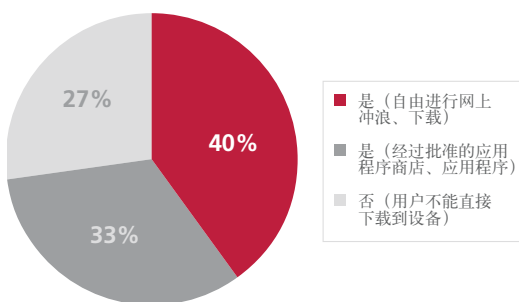
Netmedia（墨西哥的一家专门从事商业技术的独立出版公司）所有者 Monica Mistretta 表示：“除非设备属于大公司并且部署了安全策略，否则用户倾向于使用他们自己的设备完成工作任务，而且意识不到他们将要招致的风险。”

意识到移动设备会造成安全风险后，95%的企业针对移动设备制定了安全策略。但是，只有不到 1/3 的员工了解公司的移动安全策略。更糟糕的是，仅有不到半数的企业报告宣称其所有员工了解他们的移动设备访问/权限。

此外，在移动安全策略的意图和本质之间也出现了脱节。在了解所在公司的安全策略的员工中，半数以上员工会严格或非常严格地看待这些策略。但是，仅有 1/5 的 IT 部门会按照其策略进行严格约束。

事实证明，策略的制定和执行非常困难。制定移动设备策略是一项艰巨的任务 - 仅有 1/10 的受访者将该过程描述为非常容易。仅有 1/10 的受访者认为执行、监控或报告数据/设备使用非常容易。

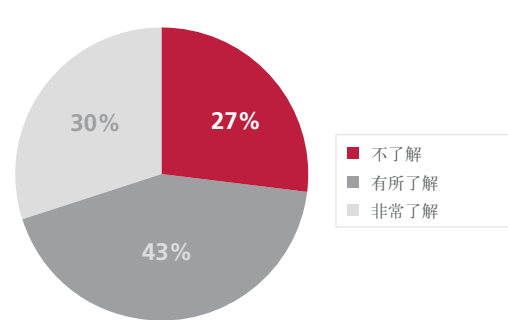
允许用户使用移动设备访问应用程序商店



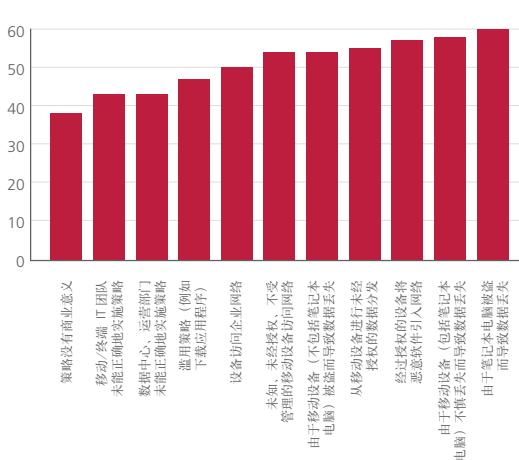
限制策略的缺失意味着潜在安全问题。四成的企业并未制定允许其员工进行同步的设备数量的相关策略。四成的企业允许员工使用其移动设备访问 Internet 并自由下载移动应用程序。1/3 以上的企业允许移动设备用户使用他们的设备连接到内部网络。

丢失和被盗的移动设备被视为威胁移动计算环境的最大安全隐患。有报道称，设备丢失和被盗是移动设备用户最普遍关注的两大问题。丢失和被盗也是大多数 IT 技术总监最担心的安全问题。

对公司针对移动设备的安全和数据保护策略的了解程度



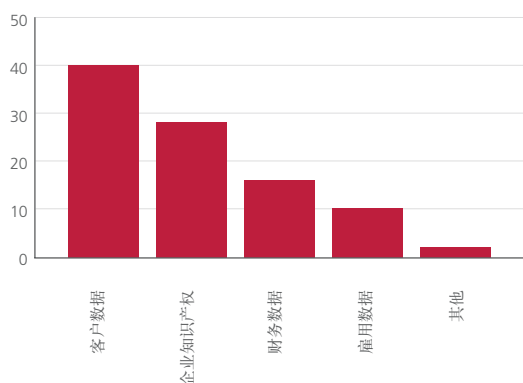
最严重的移动设备安全隐患



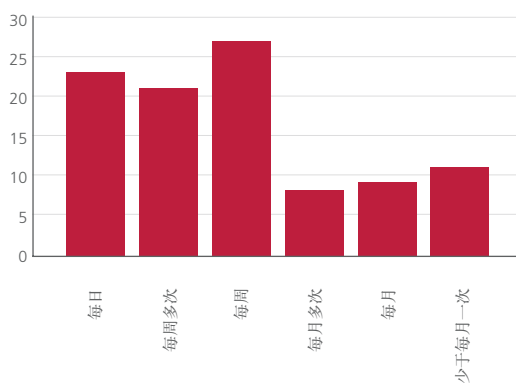
四成的企业曾经有过移动设备丢失或被盗的经历，并且半数丢失/被盗的设备中存储了关键业务数据。1/3 以上的移动设备丢失事件对企业造成了财务损失，经历过移动设备丢失/被盗的企业中有 2/3 的企业后来提高了他们的设备安全性。1/10 的企业由于预算不足，在设备丢失后并未执行进一步的安全措施。

虽然人们承认必须降低移动安全风险和威胁，但是危险行为和安全状态不佳的状况仍随处可见。只有不到半数的设备用户每周多次备份其移动数据。约有半数的设备用户将密码、PIN 码或信用卡资料保存在他们的移动设备上。1/3 的用户将工作相关的敏感信息保存在他们的移动设备上。

丢失或被盗移动设备上的数据类型



移动设备备份频率



1/5 到 1/3 的设备用户表示他们在可能出现一系列安全威胁的环境中“感到安全”。因此，约有 2/3 的用户希望使用列出的每种移动安全设施也就不足为奇了。然而，有 1/2 到 2/3 的上述用户不愿意支付这些服务，这意味着虽然他们可能购买了这些设备，但认为自己不应支付工作场所可能需要的其他安全服务。

移动设备几乎普遍用于收发电子邮件，其次用于管理联系人、进行 Web 访问以及对日历进行操作，其中 93% 的受访者使用它们收发电子邮件、77% 用来管理联系人、75% 用来进行 Web 访问、72% 对日历进行操作。



近半数用户在移动设备上存储敏感数据

	密码/PIN 码	信用卡详细信息
职业与个人信息和数据	23%	19%
仅职业信息和数据	11%	7%
仅个人信息和数据	17%	15%
不通过移动设备来使用、存储或发送此类信息或数据	49%	58%

经过长期的发展，许多从业人员将使用移动设备来完成以前在桌面机上完成的大部分工作。员工使用移动设备进行工作每天平均 2 到 4.5 小时。平均每天使用笔记本电脑 4.5 小时。印度明显高于这一水平，平均每天使用 5.9 小时。能源和公共事业也高于这一水平，平均每天使用 5.5 小时。智能手机的使用时间是每天 2.6 小时，印度也明显高于这一水平，为每天 3.7 小时，而能源/公共事业为每天 4.6 小时。

使用移动设备的工作职能部门范围很广，其中企业管理人员使用最多 (56%)，销售人员和其他移动工作人员紧随其后 (47%)。1/3 的企业允许所有员工使用移动设备。加拿大 (55%) 以及娱乐/媒体/休闲业 (64%) 显著高于这一水平。

移动设备几乎普遍用于收发电子邮件，其次用于管理联系人、进行 Web 访问以及对日历进行操作，其中 93% 的受访者使用它们收发电子邮件、77% 用来管理联系人、75% 用来进行 Web 访问、72% 对日历进行操作。

参与调查的企业的移动计算环境多种多样，用于职业目标的移动设备的范围十分广泛。至少有 1/3 的员工出于职业和个人目的使用下列四种不同类型的移动设备：笔记本电脑 (72%)、智能手机 (48%)、包括 U 盘在内的可移动介质 (46%) 和外部硬盘 (33%)。中国 (72%) 和墨西哥 (72%) 的智能手机使用率明显高于这一水平。



“设备之间分隔不明确，对公司策略缺乏认知。”



CyLab 研究人员 Patrick Tague 强调了调查结果的几个方面，重点指出移动安全和策略管理的一些明显缺陷：

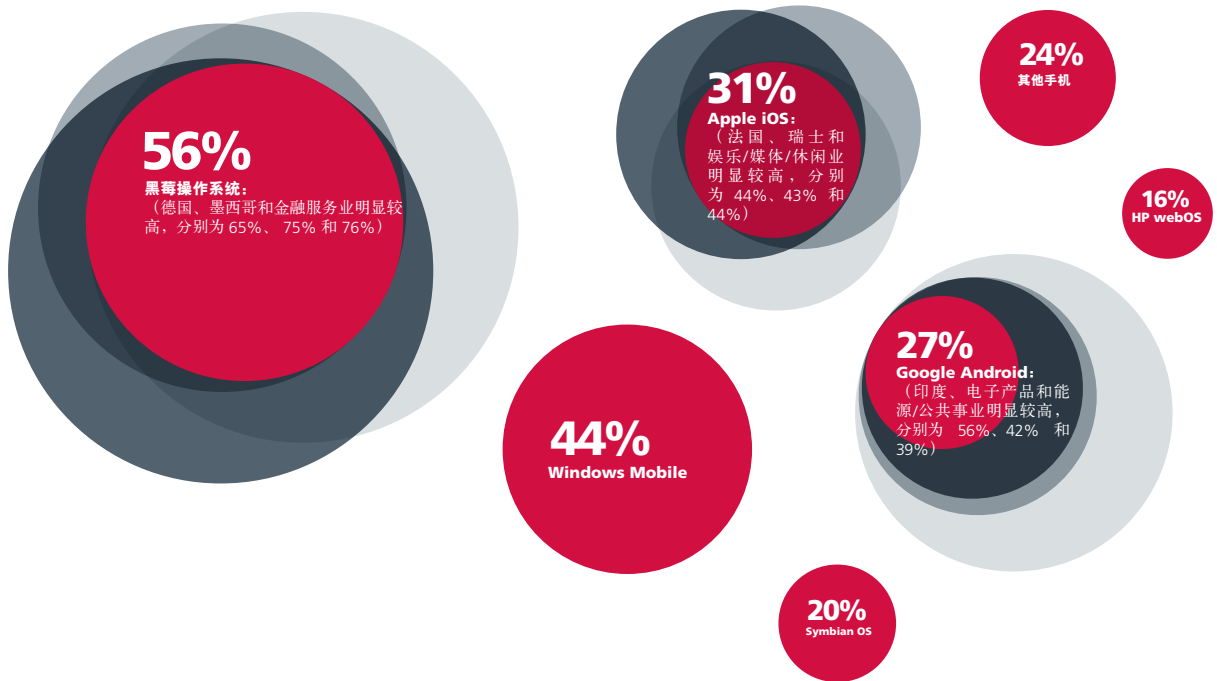
- **设备的个人使用和企业使用之间分隔不明确：** 由于设备分隔的重要性已经是多年反复存在的问题，特别是 Web 上恶意软件出现了激增，我非常希望策略制定者和管理员能够对用于企业用途的个人设备采取更加严格的策略。然而，由于确保设备可用性和策略实施所需的费用问题，因此这一结果不足为奇。
- **大多数管理员显然不愿意支付移动安全产品或服务费用：** 虽然这一结果算不上特别令人惊讶，但不幸的是，这些管理员无疑将其公司的员工和资产暴露于不必要（即可避免）的风险之下。
- **极其缺乏对公司安全和隐私策略的认知：** 除了表现出缺乏有关公司策略的内部教育或培训（这就严重限制了所有安全管理方法）外，这种意识的缺乏还暗示了其他缺点：确实缺乏策略实施（可能立即提醒管理员存在培训缺口），期望的员工行为与实际行为之间存在差距。

“我惊喜地发现，管理员正逐渐地将位置和其他上下文信息纳入安全管理范畴，” Tague 表示，“这些类型的数据为传统访问控制和身份验证机制提供了有益的补充，无疑将会提高易用性。”

虽然黑莓操作系统仍然是最受支持的智能手机平台（半数以上受访企业均支持），但其他几种智能手机也占据了很大的市场份额，并且随着 Verizon 公司采用 iPhone，我们有理由期待这些数字将在接下来的几个月里发生变化。



智能手机支持平台



“大多数企业都意识到，限制员工仅使用公司发放的智能手机将越来越困难。”

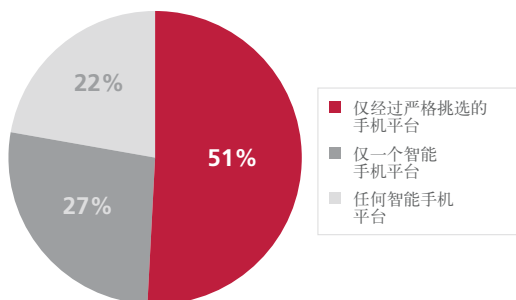
Satish Joshi, Patni Computer Systems 公司执行副总裁



“大多数企业都意识到，限制员工仅使用公司发放的智能手机将越来越困难，” Patni Computer Systems 公司执行副总裁 Satish Joshi 认为，“他们重视因允许员工自带设备而增加的安全风险，但对风险的确切性质及其潜在影响或许并不完全理解。”

当前的移动计算环境杂乱无章；在许多企业中，员工甚至将工作和娱乐合二为一。1/5 以上的企业允许在工作场所使用任何智能手机平台。近一半企业（49%）允许员工购买自己的移动设备。企业报告称，平均有近 2/3 的企业员工出于个人和工作目的使用移动设备访问其企业网络。

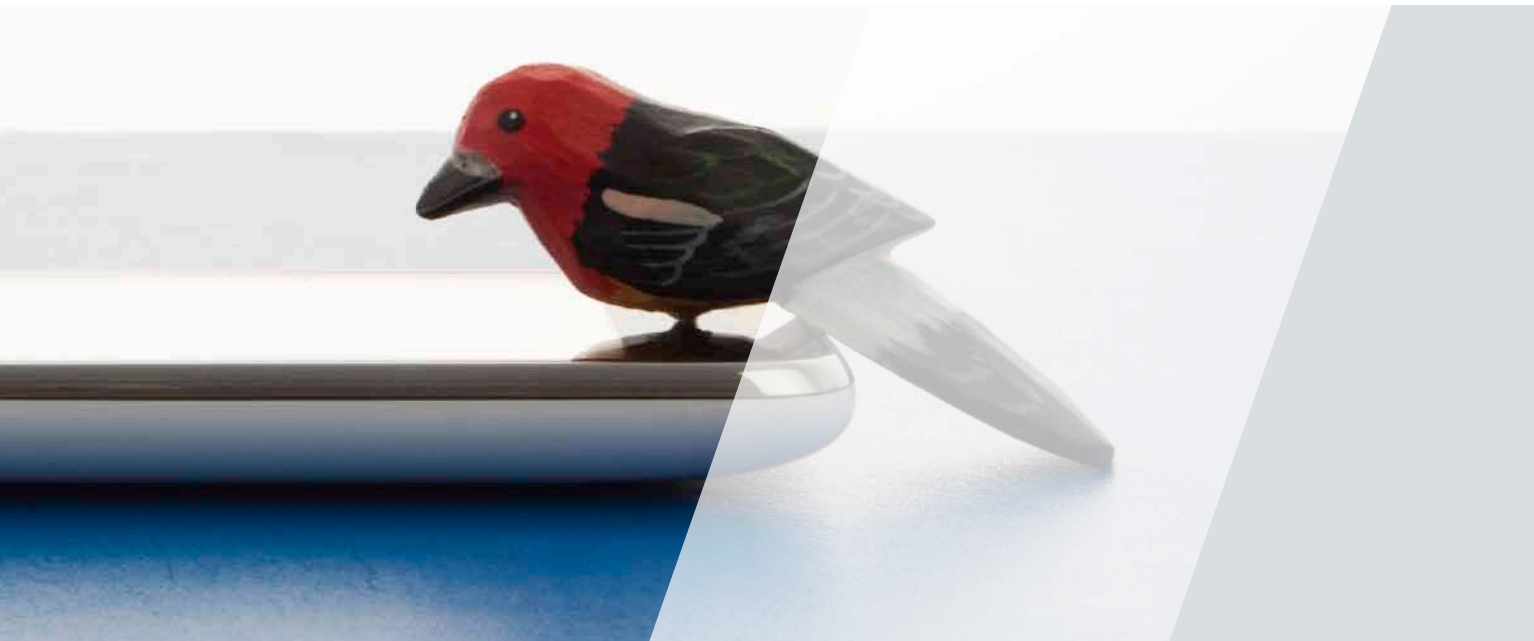
多种智能手机环境



只有笔记本电脑和上网本这两种移动设备多半由企业提供而不是由员工自行购买。约有四成的员工在不受公司管制的情况下使用个人移动设备。1/5 的员工使用企业为其提供的设备，因此企业不会对这些设备进行管理。1/4 的企业不打算分发自己的应用程序，而是鼓励员工自行下载应用程序。

CyLab 实用隐私和安全总监 Lorrie Cranor 博士强调了实现无缝安全的必要性：

“值得注意的是，我们发现世界各地有越来越多的人使用移动设备作为主要工作计算机。在美国，仍有略超过一半的受访企业将桌面计算机作为主要工作计算机，而在许多其他国家/地区，只有不到半数的受访企业将桌面计算机作为主要工作计算机。随着移动设备不断取代桌面计算机，人们可能越来越多地使用移动设备存储机密信息，因此移动设备安全问题也将随之增加。”



基于位置的技术可提高移动安全性


通过对受访者的调查，我们了解了可能对移动计算环境进一步演进而发挥更大作用的其他技术和服务。超过 1/5 的企业正在使用基于位置的技术，近半数的企业正在考虑采用该技术。

“使用基于位置的技术非常有趣，” CyLab 公司 KeySlinger (iPhone 和 Android 智能手机上的安全应用程序) 开发人员 Michael Farb 表示，“它可能会令员工失去部分隐私权利，但却能为企业提高设备的可恢复性。然而这种可恢复性只有在设备上的数据经过加密并且未被窃贼擦除或以其他方式损坏时才有效。”

CyLab 移动研究中心总监 Martin Griss 表示：“我发现目前只有 22% 的企业采用位置技术，30% 的企业甚至未考虑采用这项技术，这让我感到焦虑不安。”

CyLab 移动研究中心总监 Martin Griss 赞同移动用户位置是安全管理的重要因素这一说法。

“我发现目前只有 22% 的企业采用位置技术，30% 的企业甚至未考虑采用这项技术，这让我感到焦虑不安，” Griss 表示，“银行已经能够了解我的信用卡何时在不常见的位置或以不寻常的方式被使用，并立即尝试保护我并限制风险，而许多企业面临的风险远比我的信用卡滥用风险大得多。虽然由于大多数上下文感知产品仍然处于研发阶段，因此上下文技术（不只是位置技术）的使用仍处于早期阶段便不足为奇，但检测异常模式的简单行为监控或许能够与位置技术相结合，这一想法现在切实可行并且能够显著增强移动安全性。”



“您置身于瞬息万变的计算领域，受到用户对设备的选择以及企业对成本节约需求的驱使。”

针对企业和消费者的建议

根据与全球移动安全专家的交流，迈克菲为使用其设备连接到企业网络的企业和个人汇编了以下建议列表。这些建议旨在直接应对研究发现的五大趋势。

针对移动用户的建议

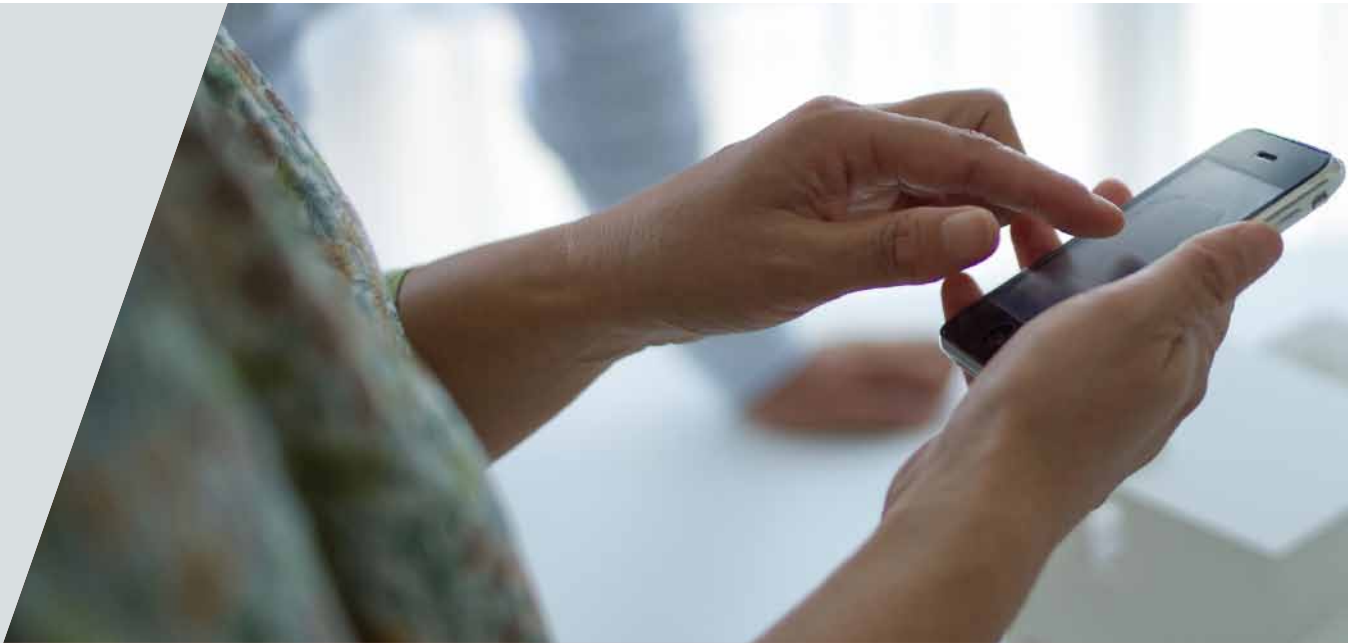
- **您置身于瞬息万变的计算领域。**随着移动设备日益取代 PC 并且几乎每种应用程序都开发了相应的移动设备版本，移动计算可以为您提供随时随地的娱乐、通信和连接。利用移动设备的优势，使您忙碌的工作更加高效。
- **受到用户对设备的选择以及企业对成本节约需求的驱使，越来越多的个人携带他们自己的设备开展工作。**充分利用企业提供的程序并使用您的技术，更快捷地进行工作。
- **熟悉企业的移动设备策略及背后的意图，确定其是否符合您的需求。**如果符合，则接受策略并坚持遵循；如果不符合，则使用两台设备 - 一台供个人使用，一台供工作使用。
- **采取措施保护您的设备。**安装防盗窃技术，并备份您的数据。将您的设备配置为在一段时间后自动锁定。不要将重要敏感数据存储在不安全的设备上，或者允许其他用户访问。
- **时刻关注移动设备威胁。**在很多方面都与置身于网络世界一样。您可能在移动设备上受到黑客攻击、感染或落入网络钓鱼陷阱，就像遭受在线攻击一样容易（甚至往往更加容易）。



针对企业的建议

- **移动技术正在将一种新型计算模式带入工作场所。**随着移动设备日益取代 PC 并且几乎每种应用程序都开发了相应的移动设备版本，移动计算可以为员工提高工作效率、竞争力和满足感。移动工作是工作场所的主要竞争优势。
- **IT 消费化已落地生根。**许多明智的公司允许、鼓励并在某些情况下提供津贴以鼓励员工使用自有技术开展工作。企业需要寻求一种以最佳方式支持、保护和管理员工自有技术的方法，从而促进成本节约。
- **用户正在改变他们对于策略的态度。**由于员工自有设备更多地关系到企业与员工之间的关系，因此企业需要根据行业、角色和现实环境，视风险情况谨慎地应用策略。
- **数据丢失和泄漏是个人和企业最为关心的问题，却没有行之有效的解决方法。**对数据分类（哪怕只是从整体粗略进行分类）并应用数据泄漏处理流程和机制，以便在尊重用户隐私的同时保护企业数据。
- **用户对移动威胁的认知仍然处于萌芽阶段。**将笔记本电脑和桌面机的安全和管理模式应用于移动设备。通过员工协议和培训对用户进行风险和威胁相关教育。

“企业必须设法保护企业数据，并在员工离职时收回数据，同时保障员工的隐私权，” 迈克菲移动副总裁 David Goldschlag 表示，“员工不再是企业的终身成员，而是通常隔几年便会更换工作的消费者。员工在进入企业工作时，会使用自己的一些设备，但在他们离开企业后，则需要归还属于公司的所有这些数据。企业需要寻求一种促进该流程的方式，同时尊重员工带入公司的‘装备’。”



总结

IT 消费化将迫使企业寻求适当方式将类似于黑莓的功能扩展到非黑莓设备。目前，黑莓不再是企业所运营的异构移动环境中的标准，因而需要投资新技术。此外，作为主要消费者的移动用户只希望携带一台设备并使用该设备连接到公司网络。这就为企业和用户带来了新的技术挑战。

“移动设备更容易被盗或丢失，但是移动连接可以使用安全机制和设备跟踪来实现移动性的安全，” Teleco（咨询公司以及巴西领先的电信信息门户）创始人兼首席执行官 Eduardo Tude 认为，“黑莓的发展就是一个很好的例子，它允许锁定智能手机和设备中的远程数据擦除。”

但它不仅是需要实施的新技术。企业还需要关注有关策略的重大问题。用户认为策略过于苛刻。因此，需要双管齐下解决策略与现实之间脱节的问题。

企业需要制定策略，但应视风险情况谨慎地运用策略。这些策略是否应该同等地适用于每个人？例如，在投资银行中，高管人员是否比证券交易员更加自由？用户需要了解其公司的策略以及制定这些策略的原因。他们必须懂得自己是公司信息的管理者，并且其自身的生计依赖于保护这些信息的安全。



企业需要将这项挑战视为端到端的挑战。设备不再是个人消费型设备或企业设备。而是两者兼而有之。设备和网络中需要兼顾移动安全性。服务提供商和制造商是必须考虑在内的重要环节，而移动设备用户则应当将安全性作为选择设备的标准之一。

设备不仅扩展了计算结构，也是用户工作和生活的延伸。用户与其个人数据的互动方式，反映了他们希望与企业数据进行互动的方式。知识工作者希望从孩子们保存足球图片的同一台设备访问他们的 Oracle、SAP 和 Salesforce 应用程序。他们需要一台集工作、生活和电子商务于一体的设备。

各种规模的企业都必须认真应对这些严峻的挑战，以便在移动计算提供的纷繁商机中获益。这些都是全球性的挑战，会影响每个国家/地区的企业和用户，并且将使得地理界限更加模糊。它又将在哪里结束？可能性无穷无尽。

设备不再是消费设备或企业设备。而是两者兼而有之。移动安全问题需要融入设备和网络。



方法

迈克菲与卡耐基梅隆大学共同合作，深入探讨移动安全和 IT 消费化这一主题。上述在线调查均由国际研究公司 Vanson Bourne 组织开展。来自 14 个国家/地区（包括澳大利亚、巴西、加拿大、中国、法国、德国、印度、日本、墨西哥、荷兰、西班牙、瑞士、英国和美国）的 1500 余名受访者参与了此次调查。参与人员被划分为两部分：移动设备的普通最终用户和具有百人或百人以上员工的公司的高级 IT 决策者。



撰稿人

Richard Power, CyLab 杰出学者

Lorrie Cranor, CyLab 实用隐私和安全 (CUPS) 总监

Michael Farb, CyLab 程序研究员

Collin Jackson, CyLab 助理研究教授

David Goldschlag, 迈克菲移动业务副总裁

Martin Griss, 卡内基梅隆大学硅谷校区主任、CyLab 移动研究中心总监

Nicolas Christin, 信息网络研究所副主任

Satish Joshi, 执行副总裁, Patni Computer Systems

Adrian Perrig, CyLab 技术总监

Patrick Tague, CyLab 助理研究教授

Eduardo Tude, Teleco 创始人兼首席执行官

Monica Mistretta, Netmedia 所有者

参考资料:

- 1 CNET, 2010 年 6 月 1 日
<http://news.cnet.com/8301-13860_3-20006526-56.html>
- 2 CNET, 2009 年 12 月 25 日
<http://news.cnet.com/8301-1023_3-10421920-93.html?part=rss&subj=news&tag=2547-1_3-0-20>
- 3 MSNBC, 2010 年 7 月 7 日
<http://www.msnbc.msn.com/id/38126866/ns/technology_and_science-wireless/>
- 4 Wired, 2010 年 8 月 20 日
<<http://www.wired.com/gadgetlab/2010/08/supercomputing-app-android/>>
- 5 CNET, 2011 年 1 月 26 日
<http://news.cnet.com/8301-31021_3-20029666-260.html>
- 6 Wired, 2010 年 12 月 9 日
<<http://www.wired.com/dangerroom/2010/12/military-bans-disks-threatens-courts-martials-to-stop-new-leaks/>>
- 7 CNET, 2011 年 1 月 19 日
<http://news.cnet.com/8301-27080_3-20028919-245.html>
- 8 Dark Reading, 2010 年 2 月 17 日
<<http://www.darkreading.com/security/news/222900775/u-s-fails-test-in-simulated-cyberattack.html>>

关于作者

Richard Power, CyLab 杰出学者, 经常发表网络安全方面的文章并进行演说。从 1995 年到 2002 年, 指导开展了 CSI/FBI 计算机犯罪和安全调查, 这项被广泛引用的调查确立了促进形成二十一世纪网络风险和威胁领域的多个趋势。

Power 是《Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace》(网络世界危机四伏: 来自虚拟空间阴暗处的数字犯罪案例)(Que)的作者, 也是《Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21st Century》(机密泄露, 财产损失: 防止 21 世纪的知识产权剽窃和经济间谍行为)(Syngress)的合著者。

关于迈克菲

迈克菲作为英特尔公司 (NASDAQ: INTC) 的全资子公司, 是全球最大的专注于安全技术的公司。迈克菲提供经实践验证的前瞻性解决方案和服务, 保护全球的系统、网络和移动设备, 使用户能够更安全地联网并在 Web 上浏览及购物。迈克菲凭借无可比拟的 Global Threat Intelligence, 为家庭用户、企业、公共部门以及服务提供商提供创新产品和强大保护, 使他们能够遵从法规、保护数据、防范破坏、发现漏洞以及持续监控安全问题和提高安全性。迈克菲坚持不懈地致力于不断寻找能够确保客户安全的新方法。

www.mcafee.com/cn

关于 CyLab

Carnegie Mellon CyLab 勇于开拓创新、富有远见卓识, 建立公私伙伴关系以开发各种安全有效、持续可靠的可测量的新技术和通信系统。CyLab 既是技术研究领域的全球领先企业, 又是信息保障、安全技术、业务和策略以及各年龄段网民安全意识的专业培训领域的世界领军者。

CyLab 基于卡内基梅隆大学 (Carnegie Mellon) 在信息技术领域长达二十多年的领先地位, 它是一项涉及六个以上不同部门和学院的 50 多个系和 100 多名毕业生的全校性计划。

www.cylab.cmu.edu/

迈克菲 (上海) 软件有限公司

北京朝阳门外大街 16 号中国人寿大厦 1709 室

邮编: 100020

电话: (8610) 85722000

传真: (8610) 85752299

上海市卢湾区湖滨路 222 号企业天地 1 号楼 1101 室

邮编: 200021

电话: (8621) 23080699

传真: (8621) 63406606

广州市天河区体育东路 118 号财富广场西塔 15 楼 106 室

邮编: 510620

电话: (8620) 38860668

传真: (8620) 38860638

销售热线: 800-810-0369 www.mcafee.com/cn

本文内容仅供培训使用, 便于迈克菲客户参考。此处所含的信息如有变更, 恕不另行通知; 信息照原样提供, 不对信息在任何特定环境情况下的准确性或适用性提供任何担保或保证。

McAfee、迈克菲和 McAfee 徽标是 McAfee, Inc. 和/或其子公司在美国和/或其他国家或地区的注册商标或商标。其他标志和商标可能已声明为其他公司的财产。本文中的产品计划、规格和描述仅供参考, 如有更改, 恕不另行通知, 并且在提供时不作任何类型的明示或默示担保。

版权所有 © 2011 McAfee, Inc.

25400rpt_mobility-security_0411

