SearchSecurity.com.cn

技术手册

一个新的安全计划

现在就更新你的安全策略，在你还没有败倒在个人智能手机的猛攻前。

- ☆ 中小企业无法藏身于杂草之中
- ☆ IT的移动化
- ☆ 安全疏忽
- ☆ Marcus Ranum和Bob Blakley的对话
- ☆ IT消费化泛滥

TechTarget
TT中国

一个新的安全计划

目 录

中小企业无法藏身于杂草之中

线上罪犯已经牢牢地瞄准小型目标。

大家好！我正在和你们说话呢。是的，你、作为一名中小企业的 IT 经理或是网络管理员。我有一个消息要通知，希望你能听清楚：已经没有足够高的杂草可以让你藏身了。

事情就是这样。

你所在的公司的规模相对较小，这使得你长久以来相信：1)你的公司不会成为黑客的目标；2)你处理和存储的信息对于因特网上的罪犯来说毫无价值。事实上，这些恰好是犯罪分子们所渴望的。他们喜欢小鱼虾。他们眼睛发亮的盯着你的公司，因为他们知道你的公司是忙碌的、人员不足并且仅仅正确地配置了网络防火墙，更别提事故响应计划了。

如此之多的入口和这么多的空闲时间可以让线上罪犯坐在那里，观察并收集信息。

现在这里我们不是讨论妈妈和流行商店。例如，我们正在讨论一个自我管理 IT 系统的大型连锁餐馆的特许经营权。介意猜一下 IT 安全对于那些特许经营权来说位于优先级列表上的什么位置么？我们正在讨论相对小型的运营，例如在不可靠

的终端销售系统上处理信用卡事务的 3 级和 4 级 PCI 商家。还有可能的是，在室内某处运行着服务器软件的有漏洞的 PC 机已连接到因特网。并且在那个有漏洞的 PC 上可能还安装有 RealVNC 或是其它远程访问管理接口（以便某些顾问或是技术专家可以每六个月登录来确认一切运作正常）。

如此之多的入口和这么多的空闲时间可以让线上罪犯坐在那里，观察并收集信息。对于网络犯罪分子来说中小企业（SMB）是一个巨大的活靶子，并且我相信 SMB 缺乏安全的情况在很长一段时间以来都是信息安全界肮脏的秘密。我们仅仅是内疚地关注引人注目的攻击事件，如 RSA、HBGray、VA、Heartland、TJX 和其它类似的事件。往好的方面说，可从这些针对大型企业的事件中吸取教训，其中一些具有无限的资源。

从这些事件中，我们看到他们都犯了简单的错误。这些事件同样阐明了数据安全以及做吸引执法部门和执法者眼球的干净利落的工作的重要性。

但是，我们在一年中会遭受一次或两次 RSA 方式的攻击的同时，每年却有数以千计的针对 SMB 的低流量攻击，且这些攻击大多数没有被发现、报告和处理。这太可怕了。

不过，最新一期的 Verizon 数据泄漏调查报告（简称 DBIR）对开始扭转这个趋势有所帮助。该报告最大的结论是：网络犯罪分子们偏好更小的、容易的目标。

有很多原因使得小型的组织们拥有很少的专门的信息安全资源。它们在安全技术上的投资是最低限度的，且安全意识也相对低。在本地最受欢迎的酒吧中，IT、特别是 IT 安全不是其核心竞争力，销售啤酒才是它的主业。

该报告回顾了 2010 年由 Verizon 的调查人员处理的泄漏事故。他们认为，尽管泄漏事故的数量在上升，但在这些事故中被窃取的记录数量在下降。为什么？这里有很多意见，最开始提到的是一些高级人物的被捕让一些顶级的地下操作者们活动放慢了。此外，在最近的十年间，已经有数以百万计的信用卡受到侵害，这个数据显然是低估的。网络犯罪分子们可能在寻找新的收入源头（知识产权？）。因此，他们开始袭击那些小型、脆弱的目标。该报告说这些目标“给犯罪分子们提供了不太稳定的数据源头”。最难得手的行业是零售业和医疗业。

报告中提到：“犯罪分子们可能在进行典型的‘风险 VS 奖励’的决定，并且从最近大范围的入侵金融服务公司后的逮捕和起诉事件来看，他们更倾向于‘安全地做游戏’”。为数众多的针对旅馆、餐馆和零售商的小型攻击代表着较小的风险，而犯罪分子们在这些目标中可以收获很多。

线上的犯罪分子们掌握着你中小企业的软肋，他们确实如此。你可能像财富 1000 强的公司那样成为定制的恶意软件的受害者（DBIR 报告中推断恶意软件的定制化费用/服务可能很低）。你同样要花费很长的时间来发现和补救泄漏事件。

例如你错误地假想你的 POS 厂商会对泄漏事件采取行动，并且当你意识到全部责任都在你身上时，这匹马——和你所有的信用卡数据——已经离开了马房。花些时间来阅读该 DBIR 报告，然后花时间来从藏身的这些杂草中走出来。

Michael S.Mimoso 是 TechTarget 安全媒体组的编辑部主任。发送对该专栏的评论到邮箱 feedback@infosecuritymag.com。

（作者：Michael S.Mimoso 译者：Odyssey）

IT 的移动化

银行和金融机构正在匆忙赶上移动化趋势，但却忽略了安全置。

人人都相信 IT 消费化是一列即将来临的火车。很多文章都描述了这种使用趋势。移动化是最新的消费化运动——大型和小型的组织正在拥抱移动化来吸引消费者的注意力并提升企业的生产率和协作性。

热衷于采用移动化的行业之一是支付及银行业。每个消费者银行和金融机构具有某些形式的移动化支付/银行业务策略。然而在没有咨询安全团队，甚至在邀请了安全团队参与讨论却根本不听取他们的意见的情形下，这些组织做出了许多关于移动银行业务的重要决策，因为每个人都感觉到移动化趋势的紧迫性。

每个消费者银行和金融机构具有某些形式的移动化支付/银行业务策略。

例如，有许多压力使得通过短信服务（SMS）推送信息。短信服务账户告警、余额查询等等正在成为习以为常的事情。在北美有一个独一无二的现象最好地形容了短信服务到 Web 服务。设想你的银行给你发送账户透支短信告警并且包含一个

URL 来让你存更多的资金。如果你点击该链接，然后你的移动浏览器跳转到银行主页。这是一个从短信服务到 Web 服务的典型应用案例。短信服务不是安全的和认证的通信媒介，并且通过短信服务发送的链接是存在问题的。骗子们能轻易地伪造一个短信，对于消费者来说在移动屏幕上来区分钓鱼和真实的 URL 是很有挑战性的。

类似地，每个人都想让移动银行与金融机构的单点登录（SSO）设施集成。确实，那样做是件好的事情。但是我知道许多短信银行业务的部署，从手机号码到用户账户的映射信息——包括用户凭证——是存储在 DMZ 中的服务器上的，从而实现有效的短信服务访问。这些部署没有经过完整的安全架构评审；一个胜任的安全架构绝对不会允许这种设计。对于短信服务器来说，正确的方法是通过一套安全的 SSO API 连接到位于内部网络的受到正确防护的 SSO 服务器。但是做出这个设计决定时没有牵涉到安全。

另一个令人不安的趋势是企业中安卓（Android）操作系统设备的快速扩增。来自 comScore 和 Nielsen 的最新统计数据都表明，安卓操作系统是现在最畅销的智能手机平台。尽管这些统计数据来自消费者的销售，但企业也目睹了安卓操作系统迅速渗入。

当许多开发人员偏好安卓操作系统时，安卓也为 IT 带来了一些任何时候都不太可能迅速解决的独一无二的安全挑战。比如下面两个：

- 市场细分化：由于安卓操作系统市场的细分化，如果你所有的安卓操作系统设备来自不同的厂家，没有一个简单的办法做一个通用的补丁来更新它们。这个问题会将终端管理一直回退到 80 年代！
- 天生缺乏对安全的支持：人们期待安卓 3 支持盼望已久的终端加密特色功能，但是安卓 3 的发布日期尚不明确。

IT 的移动化可能是无法避免的。你最好为此进行准备。但是如果你在采用和应用决策中没有考虑到安全，很可能这列即将来临的火车在到达车站前会造成一些破坏。

Chenxi Wang 是 Forrester 研究机构的副总裁和首席分析师，

在那里她从事于安全和风险职位，请发送对这个专栏的评论的邮件到 feedback@infosecuritymag.com。

（作者：Chenxi Wang　译者：Odyssey）

安全疏忽

索尼及其他数据泄漏表明，我们需要数据的问责制度和更好的配置管理。

在多次的系统数据泄漏导致其至少 1 亿客户的敏感数据暴露之后，SONY 公司设立了一个首席信息安全官职位，并正在实施额外的防火墙和其它安全保护措施。

该公司是一系列与知名度高的数据泄漏作斗争的公司之一，数据泄漏在 2011 年的头几个月让这些公司处境艰难。RSA 是 EMC 公司的安全部门，它仍在调查一个可能已经使其最珍贵的资产——知识产权暴露的数据泄漏。市场服务公司 Epsilon Data Management，负责为包括 RSA 在内的许多主要公司处理客户邮箱地址和其它信息，它也经历了严重的系统数据泄漏。

Sony 公司的高管们已为他们的安全过失道歉，并将为客户提供免费的信用监控，这是跟踪数据泄漏的一个标准措施。但是，安全专家表示，Sony 的泄漏暴露出了太多问题，包括公司无法将客户的敏感支付数据与其系统的其它数据隔离。

Sony 的初始泄漏影响到了其 PlayStation 网络的 7700 万用户。而在一周之后，该公司透露，依赖于其在线娱乐部门的一个服务器也被暴露了，该服务器可以追溯到 2007 年的信用卡信息，此次事故可能会影响到另外的 2400 万人。同时，在日本的第三次系统数据泄漏会影响到超过几百万的 Sony 客户。

专家表示，最近的数据泄漏表明企业需要对数据安全进行更好的管理。安全顾问公司 Holmquist Advisory 的总裁 Eric Holmquist 说道，很多时候，公司注重于基础架构和系统安全改善，但却不能获取存储在远程系统上的数据清单。

“我已经看到许多这样的情况，人们可以证明所有的技术、所有的程序以及所有的政策，但当你说，‘太好了，数据清单在哪里呢？’然后你就会得到茫然凝视。” Holmquist 说，“经常需要一个重大事件才能使人们把事情做得更好，这是很不幸的。”

Jon Gossels 是咨询公司 SystemExperts 的总裁和首席执行官，他建议所有公司，无论大小，都拿自身与 ISO 270002 对照。该框架可以帮助公司对其安全政策进行正式化，从而更紧密的管理他们的资产，并把操作管理、风险分析和访问控制连接起来。

“理解你的业务应该以什么方式运作以及它实际是怎么运作的，并找出两者间的差距。”

“理解你的业务应该以什么方式运作以及它实际是怎么运作的，并找出两者间的差距。” Gossels 说道。

Gossels 表示，Sony 的数据泄漏与其它公司的泄漏存在相同之处。通常情况下，各公司不会运行最新的软件。即使它们运行的是更新的软件，一个配置错误也可以引起缺陷，他说道。据 2011 年的 Verizon 数据泄漏调查报告称，几乎所有被分析的数据泄漏都利用了配置缺陷或“系统/应用程序的固有功能”。事实上，Verizon 发现，在 381 件泄漏中只有五个被利用的漏洞归咎于黑客。

参照 RSA 的数据泄漏事件， “我们发现，在当前，即使是那些在安全方面很擅长的公司也非常容易受到攻击。” Gossels 说道，“现在，有组织犯罪猖獗，还出现了敌对的外国政府以及工业间谍等事件；攻击者们正试图做一些难以发现的事情。”

在很多情况下，各组织正在做更好的补丁工作，但是极少数工作是用来解决旧系统中的软件漏洞问题，Bill Curtis 这样说道，他是 IT 软件质量协会的主管和合伙人。即使 SQL 注入、跨站点脚本以及缓冲区溢出等漏洞被找到并修补了，一个坚定的黑客也会找到他的入侵方法，Curtis 说道。他认为，公司需要对他们的系统执行一个更彻底的代码审查，同时保持一个更好的配置管理程序。

“一旦你将你的应用程序暴露在网络上，你就会与你可能不认识的人存在各种难以预料的互动，” Curtis 说，“一个支付系统不会希望被连接到一个用于游戏世界的系统。”

（作者：Robert Westervelt 译者：Sean）

Marcus Ranum 和 Bob Blakley 的对话

安全专家和信息安全杂志专栏作者 Marcus Ranum 延续了一个新的双月刊专题，在那里他一对一地与一名安全业内人士进行交流。这个月，Marcus 是和 Bob Blakley 交谈，后者是 Gartner 公司的副总裁和杰出的分析师，他负责管理身份和隐私事务，以及风险管理。

Marcus Ranum：让我们开始进入话题吧。你知道，对于在计算机安全领域我们可以管理风险这一观点，我是一个非常直言不讳的怀疑者。因为我们首先必须

理解风险，然而这项工作我们似乎并没有做好。把核事故和华尔街崩溃作为风险管理失败的例子，这样可能不公平，但是，实际上，这是不公平的吗？

Bob Blakley：你是在开玩笑，对吧？指出这些事情是风险管理的失败当然是公平的。以切尔诺贝利为例。切尔诺贝利事故确实已经导致了比切尔诺贝利核反应堆在其生命期内所创造的价值更多的费用，而这一数字在可预见的将来还会继续增加。此外，这个事故把费用强加给了这样一些人，他们与反应堆的建设毫无关系，没有从它那里得到过好处，并且也没有得到关于它的建设和经营方面任何决定的任何发言权。这是教科书里所定义的风险管理失败——即导致整个行动只呈现出净负的生命周期价值的一个事件，并且它的成本还不只限于承担这个行动的组织内。在看到这个事故的后果之后，没有一个有理智的人还会将切尔诺贝利核电厂建成它以前那样的形式。对于我们是否可以成功的管理设计如切尔诺贝利一样的核反应堆的风险这一点，（至少对我来讲）目前是尚不清楚的——尽管我们可能会比较幸运。我相信反应堆的设计（当然可以是聚变反应堆也可能是一些裂变反应堆）的风险是可以被管理的。但是这对安全来讲并不一定是好消息，因为（除了恐怖威胁）反应堆的风险不像信息安全风险——这种安全风险更严重！自然风险，比如：地震和海啸，并不分析反应堆，也不需要试图找出这些事件最坏的可能结果是什么。只有人会做这些。所以，自然风险并不是理想的最坏情况。在安全方面，我们必须总是假设我们可能需要对付一种最坏的情况。

Marcus：你所指出的这个事故导致的损失远比这一行动的生命周期价值大得多，这一点是有充分依据的。当涉及到安全时，我总是会反复不断的遇到这个问题：提倡预防为主的安全从业者正在与一个项目结果最佳情况的评价进行竞争。这是一个关于假设斗争（dueling fictions）的问题，如果一个假设是 “它将为我们节省一百万块钱并增强我们客户的安全意识” ，同时另一个假设是 “它将有可能暴露我们的客户数据库” ，我们明白哪一个假设更有吸引力。我认为安全从业者对此会更加明确。我们所说的：“人们有可能试图非法入侵系统”和“9 级地震是有可能的。” 是非常不同的。我们在说“人们试图非法入侵系统”时，是不是意味着有可能发生的事情事实上肯定会发生？

Bob： 坏人也必须养家糊口，所以肯定的是我们还会受到攻击，而且攻击者和我们一样聪明。此外，要么是他们将会得到任由他们支配的重要资源，要么是我们正在保护错误的东西。风险管理倾向于变成一个政治讨论，在这个讨论中，管理者使用诸如“可能”和“不可能”等词语来阻止受到保护的投资，而支持具有危险但有潜在盈利功能的投资。这是一个摆脱风险管理并用博弈论来取代它（至少在计算机安全方面，我们有真正的对手）的很

风险管理倾向于变成一个政治讨论，在这个讨论中，管理者使用诸如“可能”和“不可能”等词语来阻止受到保护的投资，而支持具有危险但有潜在盈利功能的投资。

好理由。这样做就把谈话从“我被陨石击中的几率是多少”转移到了“你认为坏人有枪吗？”

Marcus：几年前我读了 Charles Perrow 所著的《Normal Accidents》，被他的观点吸引住了，这个观点是：随着系统变得更加的相关和相互依存，我们预测故障模式的能力最终会消失。我不确定“连通性”的观点不仅仅是主观的做法，但是它确实听起来令人信服。不禁联想到日本核反应堆的情况：他们的自动防故障装置通常工作着，并且我们假设它原本会更加糟糕的。但是它原本也可以更好的。当两个超出你最坏情况的事情几乎同时发生的时候，你如何推断出一个潜在的系统故障呢？

Bob：我不确定我们可以认为福岛核事故原本会更加糟糕。仙台地震及其后果已经使我真正认识到的事情之一是：某些事故（包括核反应堆事故）是缓慢地发生。Solon 给 Croesus 的建议是正确的：等待，直到最后再来评价事情有多糟糕。但是，为了回答你的问题而不是对你的假设表示异议，在这里我认为我们应该如何推断出潜在的系统故障：在零阶（zeroth order）阶段，我们应该设想出事故可能导致的最坏结果，并评估这些结果。除非在此情况下我们确定我们能够阻止这一灾难，或者能够从这一灾难中恢复过来并能承担所有后果的代价，并不仅仅是应对与我们自身相关的直接后果，否则我们不应该继续建造这个系统。在完成这个分析之后，

我们可以进行一阶（first-order）考虑，比如：在控制上要花费多少钱，实施什么样的控制，如何为失败分担责任以及如何评定渎职和不称职的惩罚等等。

关于 Perrow 连通性的概念，我认为真正的事实是非线性，或者对初始条件具有极端敏感性。在复杂系统中的问题是：小的变化可以引起大的不可预测的结果，并且事件结果的数量是如此之大，以至于我们不能通过计算概率空间来找出哪些事件结果是我们需要避免的。

关于 Perrow 连通性的概念，我认为真正的事实是非线性，或者对初始条件具有极端敏感性。

Marcus：如果我们把这个理论引入到系统/网络安全方面，似乎我们已经面临了同样的问题。如果我们认为安全破坏是故障的一种形式，那么似乎我们又回到了试图基于当前期望的预测未来这个问题上来，尽管我们知道未来不一定像现在一样。我想我正逐渐回到这样的观点：一些系统不应该与其它任何东西连接在一起，就是这样，没什么好说的了。但是，实际上，那就像这句话一样荒谬，“禁止核武器，就这么回事。”事实上，秘密已经泄漏并且在自由传播。

Bob：好吧，我们不应该试图预测未来，但是我们应该知道最坏的情况。如果最坏的情况太糟糕以至于不能容忍，我们就应该改变一下。如果最坏的情况，或者许多情况，不可能被弄清楚，那么我们应该做我们能够理解的事情。你关于推断的

观点也是非常重要的，许多风险管理失败都是由“未来会和过去一样”这个假设引起的。虽然未来经常和过去相似（有时是由于深层次的原因），但有时重要的事情发生了改变，我们的假设却没有随之而变。当这种情况发生的时候，我们的模型给出的是无意义的答案，同时我们得到的是令人讨厌的例外。例如：有相当充分的证据表明：气候变化目前正在改变严重洪水的频率，这种方式使得保险单定价极其不准确。

Marcus：我觉得这就是我对计算机安全的风险管理感到真正不舒服的地方。一般来讲，被销售出去管理的最坏情况与实际的最坏情况完全不一样。所以在我们进入未来杂乱的现实之前，我开始质疑我们初始的假设是否是大致正确的。在 IT 领域，未来和过去是完全不一样的，除非你只关注它的相当狭义的方面，比如硬盘容量或者处理器复杂性。早在 20 世纪 80 年代，我们没有人意识到互联网将是很重要的事物（因为如果我们意识到了的话，我们现在会拥有属于我们自己的私人国度）。以及在 20 世纪 90 年代，我们没有人会预测到社交网络。我还会被人们急着在网上发布关于他们自身的信息惊呆了——当他们抱怨营销人员在交易这些信息时，我更是被惊呆了。像汽车保险这样的事情与长期的观察相关，观察表明比起年轻女性，年轻男性是更糟糕的驾驶员，但是互联网方面的事情与长期观察无关。

Bob：我们本来也可以就“是由安全专家、还是由社会变革来解决信息共享问题”这个话题进行一次更长的讨论，但你的观点是正确的。互联网不仅仅是一“件”新事物，它还是一“种”新事物。它是相当非线性的，而我们的大脑只进化到可以处理线性现象。我们不仅没有关于互联网的长期信息，就算我们有这些信息的话，我们甚至很可能没有合适的工具来理解关于互联网的长期信息。

Marcus：我也深切的担心：那些鼓吹潜在风险事物的人往往是那些正在对它执行成本/效益预测的人。无论你对云计算持怎样的看法，它似乎是一个元风险（meta-risky）行为，使得那些力图得到它的业务单位成为预测它会节省多少钱并洽谈服务级别协议的业务单位。这似乎令人生疑，就像让石油公司自己决定去进行深水钻井研究一样。这使我想知道在一个特定的情况下“决定”指的是什么。

Bob：外部效应是一个巨大的问题，就管理、政治以及总人口而言，它们是利益冲突和完全的技术无知。这些问题都很难解决。外部效应只能用良好的公共政策来消除。汉莫拉比（巴比伦王国国王）在这一点上比美国政府理解的更清楚。汉莫拉比这样管理他的工程师：“如果一个建筑师为一个人修了一个房子，但是没有使这个建筑足够牢固，然后房子倒塌了并导致了房主的死

外部效应是一个巨大的问题，就管理、政治以及总人口而言，它们是利益冲突和完全的技术无知。

亡，那么这个建筑师将会被处死。如果它破坏了财产，他将要修复它所破坏的任何东西，因为它未能使得房屋坚固，所以他要自己出钱重修这个倒塌的房子。如果建筑师为某人修建房屋，但是未能使得这个建筑满足要求并且一堵墙倒了，那么这个建筑师将自己出钱加固这堵墙。”

Alan Greenspan 让人们自我管理，然而当这样失败时他感到很惊讶。2008 年的金融危机后，他说：“我们这些指望贷款机构的自身利益来保护股东权益的人，包括我自己在内，都处于难以置信的震惊状态。”这也表明在 4000 年里我们倒退了多少。Greenspan 阐明了问题所在，即它是一个风险管理的失败。以下是他所说的话：

“现代的风险管理模式统治了几十年。然而，其整个思想体系在去年夏天轰然崩溃。”这也许是他唯一说对了的重要事情。

Marcus：我很惊讶，在 IT 领域，竟然没有人想到大而不倒策略。或者是不是他们已经……？

Bob：你不应该提到这点。我们不希望任何人知道这样的事情：对于解决安全性问题，我们连续的失败会保证我们终身的安全性。我们可以删掉这部分吗？

Marcus：Bob，一直以来，你谈论这个话题总是令人着迷的。我真的很感激你花费时间来指导我。当我像往常一样思考风险管理时，比起我所理解的，我感到更多的不确定性。

（译者：Sean）

IT 消费化泛滥

个人智能手机和其他计算设备正不断涌入企业，迫使关于安全的思考发生转变。

大约两年前，Thomson Reuters 公司就开始着手处理在全世界企业里普遍存在的一个问题：员工把他们的智能手机和其他一些电子产品带到工作场所中。尽管公司可以通过制定策略和使用类似于黑莓企业服务器等技术来锁定公司所拥有的移动设备，但是，对于这些个人设备我们需要一个全新的思考方式。

“我们知道，数据可能存放在我们所不能控制的设备上，需要利用类似黑莓的处理方式来管理这些设备，” Tim Mathias 说道，他是 Thomson Reuters 公司的 IT 安全高级总监。“问题是我们并不拥有设备的所有权，所以我们开始在公司内研究相关技术、策略和标准，并接受挑战，提出了一些策略，允许个人使用他们所选择的设备，同时保护公司免于风险。”

这家位于纽约的信息巨人（在全世界 100 多个国家拥有 55,000 名员工）正采用一个多层次的方法来处理这个日益严重的问题。除了制定政策，它还在调查移动设备管理技术，并与技术伙伴开展合作，从而弄清楚移动应用所带来的安全风险。

iPhone、iPad 以及 Android 设备在企业里的泛滥正在主导一次重大的转变，即越来越远离公司拥有、公司控制计算机系统的标准模式。为了提高生产力，功能强大的便携式计算系统使得员工可以随时随地访问企业电子邮件。但同时，这个 IT 消费化使得安全管理者们紧张不安。这些个人移动设备很容易丢失（比如被小偷窃取），导致保存在它们上面的所有企业敏感数据一起丢失。移动设备恶意软件以及应用程序也逐渐出现。

专家们表示，这一全新的后 PC 时代需要公司转变它们的安全思想，制定新的策略，并在不降低设备用户使用体验的情况下实施维持企业安全的技术。毋庸置疑，IT 消费化是一个企业不能忽略的趋势。

“如果你认为你可以禁止员工使用自己的移动设备，那么你是在逃避它。”要么你控制它，要么它将控制你。

“如果你认为你可以禁止员工使用自己的移动设备，那么你是在逃避它，”Philip Cox 说道，他是咨询公司 SystemExperts 的安全和规则遵从主管。“要么你控制它，要么它将控制你。”

一个成长的浪潮

这可能是许多 IT 经理都很熟悉的一个场景：一个中意 iPhone 或 iPad 的 C 级果粉主管希望企业可以对此类设备提供支持。这个趋势是在去年真正确定下来，

Ojas Rege 说，他是移动设备管理公司 MobileIron 的产品和市场部副总裁。“这导致了这样一个概念：IT 部门范畴之外的设备正在进入公司，并还需要 IT 对其进行支持，”他说道。

Citrix Systems 公司的首席安全战略家 Kurt Roemer 表示，自从 iPad 和其它平板电脑出现以后，他被那些充满担忧的企业安全经理们的电话所淹没。他们想要知道如何告诉他们的主管，在公司不能使用这些设备，但是“主管们说，‘如果你不把这个设备放在网络上，那么我会找到愿意这样做的人，’”他回忆说。

“越来越多的员工想要把他们的个人设备带到企业来，而许多企业并不乐意，但是他们正被迫对这种情况妥协，”IT 服务和解决方案提供商 Dimension Data Americas 的一位主要安全顾问 Nicholas Arvanitis 说道。

看起来，公司正在屈服于这个要求。据 Forrester Research 今年第一季度对北美和欧洲约 1,000 家各种规模企业的一项调查来看，大约一半的受访公司对员工拥有的移动电话和智能手机提供了支持。

在谈到公司如何处理个人手机和平板电脑的涌入时，Perimeter E-Security 公司的首席技术官 Andrew Jaquith 把在六个月前，当他还是 Forrester 公司的分析师时，所看到的情景比作著名的忧伤 5 阶段：拒绝、愤怒、讨价还价、沮丧和接受。

“我想说的是，大约一半的公司正处在讨价还价阶段。他们并没有完全接受它，但是知道需要做一些事情，并正开始考虑需要制定什么样的策略以及执行什么方法，”他说道。

消费者移动设备既代表了不幸又代表了机遇，Jaquith 说。“你正在使得 IT 安全重新思考其对移动设备的整个方法，在这个意义上讲，它们是一个不幸，”他说道，“但机遇是很明显的：这些设备给员工带来了更多的满足感和工作上的高效率。随着我们进入后 PC 时代，企业将被迫以某种方式来适应这些设备。”

移动威胁

对于 Thomson Reuters 公司招聘新员工来讲，支持员工拥有的设备是很重要的，Mathias 说。在致力于制定个人移动设备策略的两年里，可供选择的技术已经得到了提高，该公司对这些设备所带来的风险的理解也有所增加，他说道。

“简而言之，能够把 Android 手机连接到我所选择的任何工作站上，并使用手机存储器把文件带出办公室，可以将这些手机当成一个巨大的 USB 设备。”

“简而言之，能够把 Android 手机连接到我所选择的任何工作站上，并使用手机存储器把文件带出办公室，可以将这些手机当成一个巨大的 USB 设备，”他说道。

数据丢失和未授权的安全访问是个人移动设备对企业最大的安全风险，Matthew Todd 说道，他是位于美国加州 Palo Alto 的独立投资顾问 Financial Engines 公司的首席安全官和风险与技术运营部副总裁。

“与笔记本电脑相比，诸如智能手机和 iPad 等便携式设备的确更时髦，它们更小，更有趣，但是就像老的 ThinkPad 一样充满了信息，”他说道。“便携式设备可以存储通讯录、电子邮件、机密附件，甚至是机密的图片、音频或视频。当你的智能设备与公司环境结合在一起，并且你的智能平板或智能手机可以访问内部系统或网站的时候，所面临的安全威胁将呈现出一个全新的情况。”

而更严重的风险是这些小型便携式设备很容易落在出租车和餐厅里，以及被小偷窃取。

移动恶意软件是另一个风险，但是它只是刚刚冒出来。在 3 月，Google 从其 Android 市场上删除了 20 多款免费的应用程序，因为它们包含了隐藏的恶意软件。名为 DroidDream 的恶意软件试图得到智能手机的 root 访问权限，从而查看敏感数据以及下载更多恶意软件。

DroidDream“表明了恶意软件对 Android 的威胁是真实存在的，” Chenxi Wang 在最近的报告中写道，他是 Forrester Research 公司的副总裁和主要研究员。“可以自由下载任何应用程序的个人设备是一个成熟的感染源。随着

Android 超越 iOS 成为最畅销的移动平台，防御移动恶意软件将是越来越重要的 IT 事务。”

应用程序安全公司 Veracode 的共同创始人和首席技术官 Chris Wysopal 表示，iPhone 对于恶意软件已经有相当的有抵抗力，“因为这款设备拥有已知应用程序的运行围墙，或者说白名单，增加了它的安全性。”与 Apple 公司的具有更高审查标准的软件应用商店相比，在 Android 市场上的应用程序缺乏安全审查，他说道。今年初，Veracode 推出了一项移动应用程序验证服务。

“我认为移动设备将会是下一个巨大的威胁源。我们仍然处在学习阶段，但是我认为今后它们真的会成为一个巨大的攻击目标。”

“一个最大的风险是用户安装了没有经过审查的应用程序，”Dimension Data 公司的 Arvanitis 说道。

“我认为移动设备将会是下一个巨大的威胁源，”Ryan Laus 说，他是美国密歇根中央大学的网络管理员。“我们仍然处在学习阶段，但是我认为今后它们真的会成为一个巨大的攻击目标。”

便携设备策略

尽管 Thomson Reuters 公司想要在员工拥有的设备上实施强大的安全措施，但是公司知道要做到这一点需要策略。

“我们希望能够找到并注销一部被盗或者丢失的手机，就像现在我们用黑莓能够做到的那样。但是，作为一个公司，我们需要在不属于我们的设备上拥有这样做的权利以及能够这样做的技术。这就是策略起作用的地方。在我们可以开始管理这样的设备之前，我们需要同员工达成一个协议。” Mathias 说道。

Jaquith 表示，公司需要与员工之间建立一个所谓的“移动接入和安全协议”。“如果你有一个雇主和员工之间的协议，那就是说，‘你可以把移动设备带到工作场所并使用它，但是作为交换，我将会要求你做一些事情。’”这包括允许在你的设备上实施强制公司密码设置的安全策略，以及当需要在设备上执行取证或者遵从传票调查时，同意将设备交给公司负责人员。

Arvanitis 说公司策略可以列出哪些移动平台是被支持的以及根据员工的角色可以包括不同的规则。“与数据流和数据安全性一道，人们需要了解那些使用情形，”他说道。“只有你已经在企业的适当位置获得了这个安全架构，你才能实施技术控制。”

在她的“管理在工作场所的个人设备的安全和风险的挑战”报告中，Forrester 公司的 Wang 概述了应该包括在企业移动策略里的基准事项（查看“道

路规则”）。规则指出，安全团队需要与法律和隐私部门一道工作，同时也需要考虑一些由办公室里的个人拥有的设备所造成的独特的法律和隐私挑战，她建议说。

例如，她指出，如果一个员工在他的个人设备上误用了受版权保护的材料，那么企业是有责任的。另外，把企业控制强加于个人智能手机和其它设备上会与隐私法律冲突；一些国家不允许公司审查个人设备的网络安全性，执行可接受的使用策略或者强加一个终端代理，Wang 在她的报告中说道。

“对于一个全球企业，你的运营必须遵从多个、不同的隐私规则，想要知道如何监管和控制你的网络上的个人设备的确是一个挑战，”她说道。“它也可能意味着你必须针对不同的地区制定不同的策略。”

安全控制

当涉及到在一个移动设备上执行诸如密码和锁定等企业安全时，黑莓平台是最好逃脱的，专家们说道。Mathias 把黑莓企业服务器称为“黄金标准”。

“黑莓是被构建来完全地满足这些要求。它是一个发现了进入消费者世界方式的企业设备，” Veracode 公司的 Wysopal 说道。“进入企业的其他设备是来自消费者世界并且缺乏这些功能的。”

企业可以对员工在工作时使用的所有 iPhone、Android 以及其它设备，获得一个基础级的控制方法，通过 Exchange ActiveSync 来实现，专家们说道。“这将是你的瓶颈点，” Jaquith 说道，如果多次输入错误密码，那么公司可以用它来执行密码策略和设备锁定。

然而，当试图管理个人设备时，公司使用 Exchange ActiveSync 会遇到可扩展性问题，Wang 指出。一个移动设备管理系统“可以在设备上强加针对这些设备制定的任何策略，监管它们的操作，并给你一个可以把控制强加于适当范围的平台。”她说道。

随着“移动计算从仅仅是电子邮件转移到移动应用程序”，移动设备管理系统将会变得更加重要，Jaquith 说道。

据 Gartner 公司称，移动设备管理软件市场正在飞速发展，已有超过 60 家供应商，但缺乏一致性。多数供应商提供本地的或者基于软件即服务的工具并提供一系列功能，包括库存管理，软件分布与安全，诸如强制的密码、设备擦除以及远程锁定，Gartner 公司的分析师在一个最近的报告中这样写到。

他们还提醒企业：一些设备平台由于其设计上的原因会在可管理性上造成限制；公司不应该期望移动设备管理系统以同样的方式来支持每个平台。另外，据

Gartner 公司称，Android 支持仍然是不成熟的，它预测至少还需要一年，Android 才会被移动设备管理提供商很好地支持。

Mathias 说：由于移动设备操作系统更加成熟且有更好的支持能力，因此 Thomson Reuters 公司对移动设备管理供应商已经另眼相看。公司也正在寻找提高把设备连接到交换环境的能力的方法，同时通过致力于部署一个移动 VPN 功能来保护其内部环境，这个功能将与公司的数字认证部署结合，所以数字认证可以部署到实现安全 VPN 访问的移动设备中。

Research in Motion (RIM)公司最近宣布了在今年末发布一个其黑莓企业服务器的多平台版本的计划，承诺为企业提供另外一个管理 IT 消费化趋势的方法。RIM 公司正在收购 Ubitexx 公司来研发这个产品，它说将会把安全设备管理并入到 Android 和 iOS 设备。RIM 指出，公司可以“依据不同设备平台功能，期待一系列安全性、可管理性以及控制。”

专家们说，一些公司正在用来平衡移动性和安全性的技术，利用的是 Citrix 公司的桌面虚拟化技术。这样一来，没有任何企业数据会存储在那个设备上。Citrix 公司的 Roemer 说，Citrix 接收器，为包括 iPhone 和 iPad 在内的各种移动设备所提供的，充当了一个“应用程序和桌面虚拟化的窗口。”

预先计划

了解移动应用程序中的风险，尤其是那些在 Android 和 iOS 手机中的风险，是 Thomson Reuters 公司正在通过与一家公司合作来解决的另一个方面，这个公司可以扫描应用程序来发现问题。

Mathias 说，人们开始讨论是否想要拥有一个移动手机应用程序的白名单，但是白名单可能有问题，因为它使得设备的个人化少了。了解那里有哪些应用程序，移动员工是如何使用它们的，以及这些应用程序可以被怎样误用是新的知识领域。

“我们正刚刚开始谈论我们如何及时跟上这一点，”他说道。

（作者：Marcia Savage　译者：Sean）