

## BYOD 和移动威胁不断增加，企业数据安全能否跟上脚步？

非官方中文译文·安天技术公益翻译组 译注

简译版

文档信息			
原文名称	As BYOD Adoption and Mobile Threats Increase, Can Enterprise Data Security Keep Up?		
原文作者	Sue Poremba	原文发布日期	2019 年 1 月 24 日
作者简介	Sue Poremba 从 2011 年开始撰写文章，专长是网络安全和技术领域。 <a href="https://securityintelligence.com/author/sue-poremba/">https://securityintelligence.com/author/sue-poremba/</a>		
原文发布单位	Security Intelligence		
原文出处	<a href="https://securityintelligence.com/as-byod-adoption-and-mobile-threats-increase-can-enterprise-data-security-keep-up/">https://securityintelligence.com/as-byod-adoption-and-mobile-threats-increase-can-enterprise-data-security-keep-up/</a>		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。</li> <li>本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。</li> <li>译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。</li> <li>本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。</li> </ul>		

## BYOD 和移动威胁不断增加，企业数据安全能否跟上脚步？

Sue Poremba

2019 年 1 月 24 日

虽然大多数安全专家已经开始接受“自带设备”（BYOD）策略，但是领导层仍然对员工的个人电话、平板电脑和笔记本电脑的数据安全性缺乏信心。

Bitglass 公司最近的一项研究发现，由于数据泄漏、非授权 IT 系统的使用和未经授权的数据访问等安全问题，接受调查的 400 名 IT 专家中有 30% 对采用 BYOD 犹豫不决。随着《通用数据保护条例》（GDPR）和其他数据隐私法规的全面生效，监控和保护移动设备上的企业数据比以往任何时候都更加重要。然而，BYOD 仍然是网络访问的重灾区，特别是考虑到新端点的快速增长。

这引发了一个问题：相比于员工刚开始携带个人设备时，如今的 BYOD 安全性是否更好了？

### 企业更多地接受个人设备

不久前，企业领导层对员工使用个人设备进行工作的想法犹豫不决。虽然员工一直在使用他们的个人电脑和笔记本电脑访问公司网络；但是，直到智能手机和数字平板电脑推出，BYOD 的概念才流行起来。当时，这些设备的安全性还不是很成熟，IT 和安全决策者也有充分的理由担忧。

当然，在过去的十年中，手机已经发展成为个人手持电脑。Comscore 公司称，在 2009 年只有 17% 的消费者使用智能手机；而到了 2016 年，这一比例已经增长到 81%。这种不可逆转的趋势，以及物联网（IoT）和可穿戴设备的崛起，使得个人技术与企业网络密不可分。

员工认为，使用其自选的设备，以及其青睐的软件和应用，会提高他们的工作效率和产出。显然，领导层也认同这一点：Bitglass 研究发现，85% 的公司现在不仅允许员工，甚至允许承包商、客户和供应商使用个人设备访问企业数据。尽管如此，仍有超过一半的受访者认为移动威胁变得更加糟糕了。

## 移动威胁不断增加，但是安全措施并未发生太大变化

鉴于工作场所中移动设备的普遍性和相对不安全性，犯罪分子瞄准它们并不奇怪。威胁源可以先攻破一台易于破解的设备，然后利用该设备访问公司数据和个人数据。在 Bitglass 调查的企业中，超过一半部署了基本的移动安全保护措施，例如远程擦除和移动设备管理工具。此外，许多安全团队缺乏对个人设备使用的应用的可见性。

《连线》杂志援引移动安全专家凯伦·斯加佛恩（Karen Scarfone）的说法称，攻击移动设备的大多数威胁源旨在获取用户口令。

她说：“很多人重复使用简单的电子邮件口令，这是一个严重的问题。”

口令是开启“数据城堡”的钥匙，而移动设备上的口令大多没有进行加密。再加上严重的密码重用问题，这意味着威胁源可以通过个人设备几乎无限制地访问公司网络。

显然，在移动安全方面企业还有很大的改进空间。2015 年，在《网络安全法案》的要求下，美国国土安全部（DHS）进行了一项研究。研究发现，虽然联邦政府对移动技术的使用正在改善，但是“许多通信路径仍未得到保护，导致整个生态系统容易受到攻击。”

私营部门也存在类似的安全漏洞。SyncDog 公司称，对企业网络来说，移动设备是最危险的入侵点。特别是在大型企业中，“移动设备被视为安装有游戏的玩具，它们的保护与应用程序管理、网络安全、主机和其他 IT 问题紧密相关。”

## 采用智能策略保护 BYOD 安全

首席信息安全官（CISO）和 IT 领导者如何确保员工以智能、安全的方式使用他们的个人设备呢？首先，确定员工是否需要使用个人设备进行工作。如果其工作不需要定期访问公司网络，或者他们远程工作，那么他们的设备既未获得授权也未受到持续监控，因此不应允许他们参与 BYOD 计划。

其次，应该要求（或者至少是高度鼓励）员工更新他们的设备软件，尤其是操作系统和安全软件。考虑要求所有使用个人设备的员工安装公司的安全软件，并使用公司的安全协议连接企业网络。

第三，向员工传达 BYOD 策略，并采取有效措施加以强制执行。这些策略应包括最基本的数据安全最佳实践，例如实施多因子身份验证（MFA）、创建强大且唯一的口令、使用

公共 WiFi 上的虚拟专用网络 (VPN)，以及使用生物识别措施锁定设备等等。除了保护企业网络，这些措施还有助于保护员工设备上的个人数据。需要注意的是，如果不执行这些策略，那么它们就是毫无用处的。如果员工发现不遵守规则不会带来任何后果，他们将会违反规则。

在提高员工生产力方面，采用 BYOD 是有好处的。但在一个网络威胁不断增加、且数据丢失可能导致巨额罚款和声誉损失的世界中，企业需要优先考虑其关键资产的安全性，以及访问这些资产的数千个端点的安全性。

欲了解更多信息，请阅读 IBM 白皮书《自带设备的十条规则》。

## 安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：<http://www.avlsec.com>