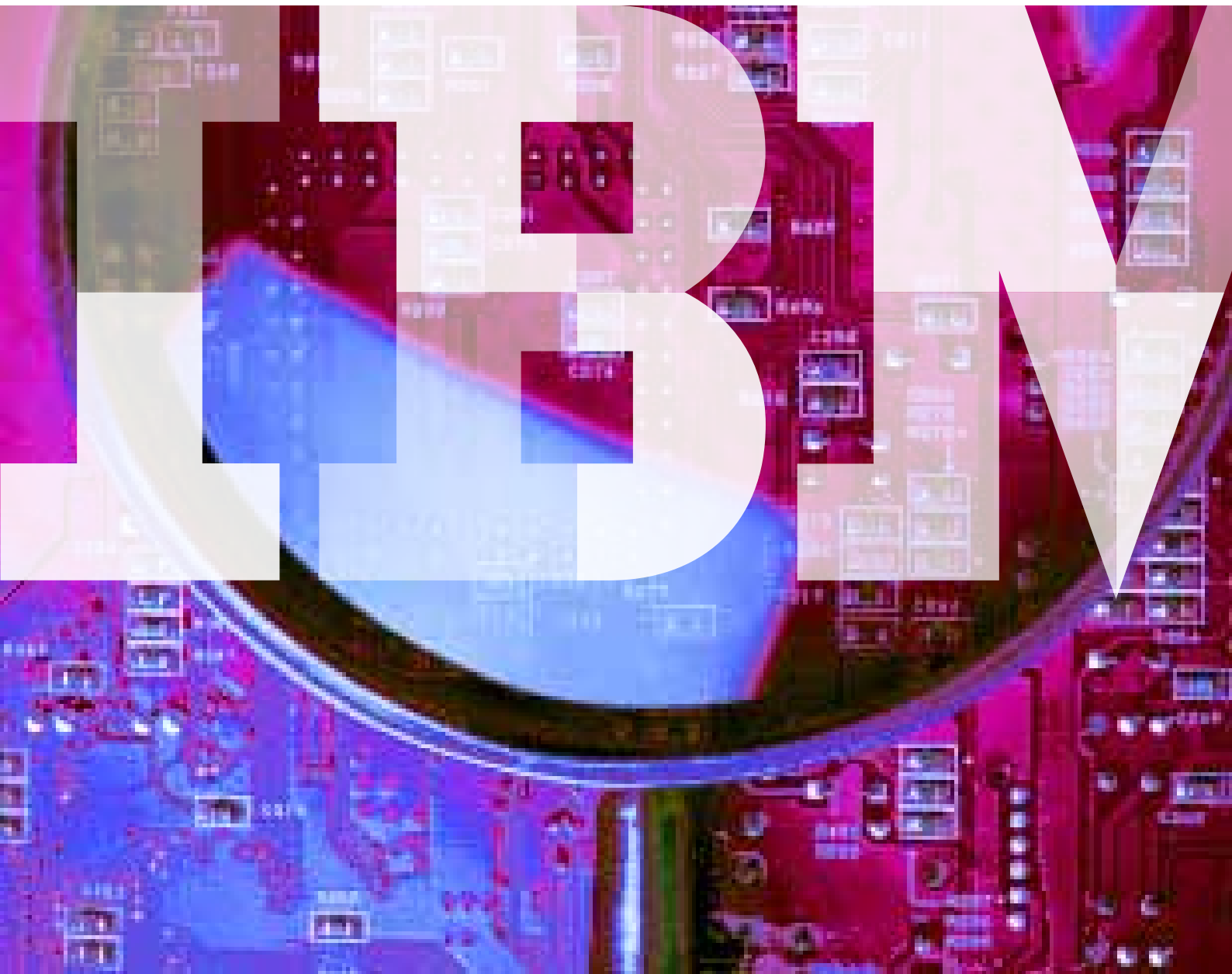
IBM全球企业咨询服务部
执行报告

战略与转型

IBM商业价值研究院

新出现的安全性趋势和风险



IBM商业价值研究院

在IBM商业价值研究院的帮助下，IBM全球企业咨询服务部为政府机构和企业高管就特定的关键行业问题和跨行业问题提供了具有真知灼见的战略洞察。本文是一份面向决策层和管理层的简报，是根据该院课题小组的深入研究撰写的。它也是IBM全球企业咨询服务部正在履行的部分承诺内容，即提供各种分析和见解，帮助各个公司或机构实现价值。

有关更多信息，请联系本文作者或发送电子邮件到：ibvchina@cn.ibm.com

请访问我们的网站：http://www.ibm.com/cn/services/bcs/iibv/

作者：Jack Danahy，John Lainhart，Eric Lesser

就IT安全性而言，2011年是引人注目的一年。数据损失的频度和范围、“分布式拒绝服务”攻击(它能够阻止合法用户访问某项服务)以及“社会黑客行动”(利用计算机网络从事社会或政治方面的抗议)凸显了在联系日益紧密的世界中进一步保护资产的需要。由于我们不可能完全回避支持连接的新技术，企业管理人员可以通过以下途经应对新出现的安全性风险：构建前瞻性的安全性智能能力；开发包括移动设备在内的涵盖所有端点的统一视图；在数据库层次上保护信息资产；以及建立更安全的社交习惯。

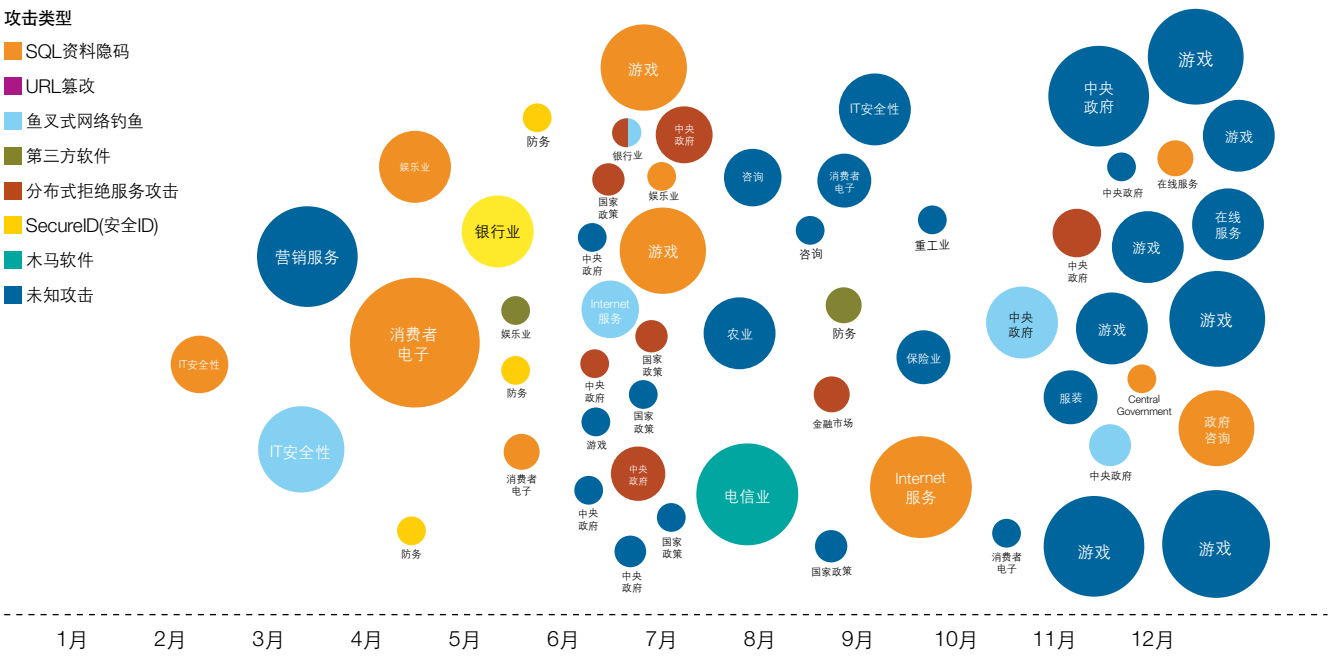
2012年IBM全球CEO研究揭示出，企业领袖们认识到，我们新的互联时代正在从根本上改变他们与雇员、客户及合作伙伴的关系。[1] 随着个人和组织机构成为联系更紧密的、更加开放的、移动性更强的、社交程度更高的商业形式的一部分，一些滥用这种联系的方法也被发明出来。攻击目标不仅限于信息技术和基础架构，个人用户也成为被攻击对象。结果，安全性不再是一个局限在信息技术专家圈内的话题。相反，在这一新环境中实现有效保护需要组织机构中各个层次上的人员充分理解相关问题并时刻保持警惕。

过去若干年里流行的许多传统的安全性威胁还在继续演化和扩散。

IBM X-Force是一个由漏洞研究人员组成的团队，它持续监控和分析世界各地的安全性威胁并每年发布两次其研究成果。[2] 这些丰富的数据为网络空间目前的问题和挑战提供了独特的、第一手的观察。这些数据不仅对IT专业人员有重要意义，而且对高级业务管理人员也同样非常重要。

2011年，大规模的网络安全性漏洞频繁出现，造成广泛的客户数据泄露，使得许多web服务无法访问，并导致数十亿美元的损失。这些事件几乎没有放过任何一个行业或部门：执法部门、政府部门、社交网络社区、零售业、娱乐业、银行业以及非赢利机构都曾经报告遭受明显攻击(见图1)。

在本报告中，我们将讨论直接影响组织机构的多个具体威胁，并就高级业务管理人员能够采取的预防性行动提出一些建议，以期改善他们的总体安全性状态。



注：圆的大小代表了漏洞的影响，以对业务造成的损失代价为标准。资料来源：IBM X-Force研究和开发。

图1. 2011年安全性事件抽样，按照攻击类型、月份及影响进行划分。

新出现的安全性问题

传统的攻击正在变得越来越复杂

过去若干年里十分流行的许多传统的安全性威胁仍然在继续演化和扩散。在多次最引人注目的事件中，包括由匿名者和LulzSec等组织发起的攻击中，都涉及到使用“SQL资料隐码”攻击，这是一种在1990年代首次开始流行的技术。[3]

这些攻击以存在漏洞的数据库为目标，规避认证机制，访问数据库中的专有内容，甚至损害托管此类数据库的操作系统。虽然许多组织机构都已经采取措施保护那些提供对此类数据库进行访问的基本web应用，但对这些系统及其支撑数据库的更新和修正却经常未接受相同程度严格的审查。

另一种一直在演变的攻击是“钓鱼”，即攻击者诱骗某些人泄露其银行帐户和身份号码等个人信息。过去，钓鱼者把这些人引导至名称与知名公司相似的网站，从而欺骗后者泄露其私人信息。

而现在，钓鱼者则直接攻击合法网页，然后在其中插入危险的子域网页。这进一步提高了信息请求的想象合法性，使得不具疑心的用户更有可能访问。钓鱼攻

击还利用了从社交网站公开获得的信息，从而针对潜在受害者捏造出一些个性化的消息，这种有针对性的攻击经常被称为“鱼叉式钓鱼”。

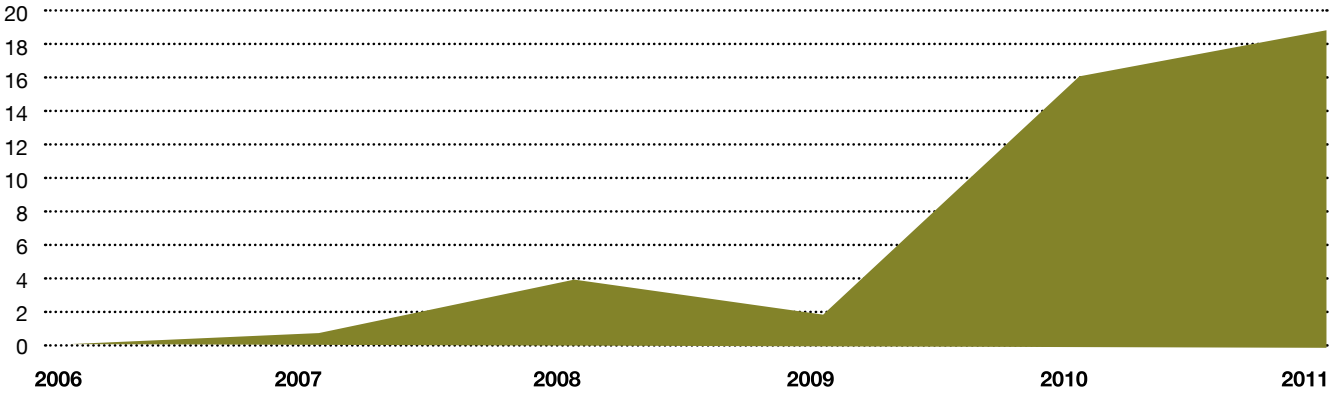
一种越来越常见的技术是利用具有破坏性后果的程序模仿合法应用。MacDefender是一套特殊形式的恶意软件，它把自己伪装成合法的反病毒程序。该程序安装之后，它假装扫描计算机，然后随机把一些文件标示为恶意程序，使得该系统看起来遭到了严重感染。随后，该恶意软件建议用户付出一笔许可证费，以便删除所标识的文件。如果用户选择了此选项，那么，用户就需要在一个网站上注册，在此，其信用卡

信息被收集并被扣费。其他的一些入侵程序，例如Flashback，则假装模仿Adobe Flash等合法程序；在被下载之后，它们就会把非法代码注入到应用中，并引导用户访问他们并未打算访问的网站。最近的一项研究表明，超过50万Mac用户已经感染上了这种Flashback病毒的变种。[4]

把你设备之外的东西带入工作环境中

过去一年，移动设备的泛滥已经明显影响到组织机构。组织机构不但需要制定移动战略来满足客户的需求，它们也需要为雇员采取一些新策略。随着越来越多的人希望利用新一代平板电脑和智能手机的强大威力，个人设备在公司环境中的使用量将会持续增长。

虽然“自带移动设备”的趋势能够为最终用户带来极大的方便，但缺乏公司所有权和控制力也给组织机构带来必须解决的安全性挑战。2011 X-Force报告特别强调，以此类移动设备为目标的恶意活动出现了明显的上升趋势(见图2)。



资料来源：IBM X-Force 研究和开发。

图2. 移动操作系统滥用，2006-2011年。

由于众多原因，移动设备带来更深层次的问题。鉴于电话最终用户、电信公司以及移动操作系统供应商之间的微妙关系，漏洞可能会在相当长的时间内不被发现。这为攻击者留下了更大的机会窗口。

此外，越来越多的移动平台和日益严格的监管要求会使风险加剧。支持“越狱”的程序(即在设备上安装未经批准的第三方应用)已经使得非法个人更易于访问手机上的数据。最后，移动设备经常把GPS硬件与语言、消息和数据服务组合到一起，这可能带来另一种攻击风险，即监控用户私人通信的多个方面 - 包括记录位置、短信、电子邮件及电话呼叫。

与针对传统工作站的大量攻击活动相比较，移动平台相关的攻击活动数量还相对较少一些。但在未来，我们预计会看到更多的安全性问题随着快速普及的移动设备而出现。

社交媒体风险：我们是否未经验证而轻信别人？

在过去若干年中，社交媒体已经从一种边缘活动跻身为世界上最活跃的在线活动。截至到2011年末，大约有80%的全球在线用户(超过10亿人)在使用社交媒体。[5] 这种增长速度为欺诈创造了新的温床，它们曾经在电子邮件中大行其道，现在利用此新环境又复活了。

社交媒体还带来了另一个维度的风险：用户倾泻到社交网络中的大量隐私信息已经改变了，而且简化了社交情报收集的方式，从而带来了更完整的个人及网络景象，而这更易于受到攻击。与遭受黑客攻击的组织机构相关的个人可能会发现，他们是在与其社交网络中遭到破坏的账户打交道，从而无意中暴露了信息或者访问了某些网站，而这些网站随后又以恶意软件感染他们。这可能最终导致公司数据资产失窃或受损。个人信息也可能成为攻击目标，以期获取密码、确定敏感文档的位置，甚至在整个组织机构中传播恶意文件。

当今不断演变的世界中的安全性

移动性、社交媒体以及web商务非常清楚地强化了一些重要观念，它们正在重塑组织机构在当今商业环境中开展竞争的方式。虽然从定义上看这些活动带来了某些形式的风险，企业的正确做法是设法减轻这些风险，而不是企图完全避免接触新一代的各种技术。根据IBM与各种组织机构打交道的经验，我们发现企业高级管理人员有四个机会来解决这些新出现的安全性问题：

- 建立前瞻性的安全性情报能力；
- 为包括移动设备在内的所有端点建立统一的视图；
- 在数据库层次上保护信息资产；
- 在保持社交关系时要保证安全。

组织机构面临新的安全性问题：攻击日益复杂；移动设备越来越多地成为攻击目标；社交媒体成为欺诈的新温床。

建立前瞻性的安全性情报能力

在过去几年，攻击次数的增多、计算设备的膨胀以及数据的爆炸都为安全性从业人员带来了严峻的挑战。甚至要侦测到已发生的入侵都是件困难的事情，从而使组织机构可能在长达数个月的时间内无法意识到其已经暴露在攻击的枪口之下。虽然企业经常能够掌握原始数据，但他们常常缺乏探测问题的可视性及分析能力。2011年Verizon数据入侵调查报告总结说，在69%的入侵中，有确凿的入侵证据存在于组织机构的日志文件中，但却极少被发现，因为数据源非常多，而整合能力又非常差。[6]

因此，目前的威胁检测取决于两个要素：在数十亿个数据点中发现可疑活动，并把浩繁的可疑事件浓缩一幅可管理视图以抓住真正要害事件。这就有必要在整个安全性运营范围内采用实时分析能力。例如，通过分析数据包流动并监控用户的异常活动，组织机构能够协助寻找到某些模式，它们可以指示出潜在的内部人员数据偷窃或者由外部实施的损害。

这种在多个数据源中进行有意义的分析的高级能力被称为安全性情报。它在四个方面不同于传统的安全性措施：

- **对流分析能力的运用** – 过去，来自设备、应用、服务器及基础架构服务的日志为组织机构提供了所发生活动的后视图。现在，高级分析能力可以提供当前的、实时的洞察，使用者可以看到用户行为、社交媒体利用情况、移动设备活动、云活动等方面的信息。
- **预测性分析能力以及对滥用预知能力** – 更好地了解错误配置的设备以及未修补的漏洞，能够让组织机构在漏洞被滥用之前即发现、优先安排并系统地解决各种风险。
- **异常探测** – 传统的安全性工作把重点放在保护组织机构免受已知威胁的影响上，例如，防范已经公开发布的漏洞以及常见的恶意软件。现在，一些高级攻击者开发了有针对性地滥用尚未披露的漏洞的方法，被称为“零日攻击”，因此，安全性团队也需要集中精力于那些超出预料或预定义范围之外的活动和行为。
- **易于部署和安排人员** – 为了充分利用新获得的安全性情报洞察，安全性团队依赖于仪表板以及其他形式的数据可视化，从而更容易地整合各种数据源并及时发现威胁。

为包括移动设备在内的所有端点建立统一的视图

鉴于形形色色的个人设备日益泛滥，而且在工作环境中使用这些设备的趋势日益明显，以更完整的方式管理它们的能力就变得越来越关键。

对许多组织机构而言，它们在使用不同的安全性平台管理不同类别的设备(例如，智能电话、笔记本电脑或者平板电脑)。虽然可以把完全不同的管理系统整合到一个单一的企业风险控制台中，但更容易、更可能取得成功的途径是由单一的基础性框架加以支持。当数据被整合到单一的平台中时，也更容易分析和响应安全性威胁。得到良好定义和控制的安全性策略能够在各个端点之间实现一致的管理，选择适当的技术并监控整个企业的安全性场景也有助于实现这一效果。

在数据库层次上保护信息资产

虽然日益增多的个人设备和最终用户系统占用了企业风险管理的时间和注意力，但数据库服务器将仍然是主要的风险入侵目标。当在攻击过程中有多个系统被常规化突破时，必须记住，攻击的终极目标通常总是有价值的知识财产、可识别的个人信息、信用卡数据以及组织机构掌握的其他类似信息。

如果企业想有效地管理这一风险，他们就需要考虑三个主要问题：数据位置、业务控制以及监管合规性。

首先，组织机构需要识别出关键数据的位置以及它们在机构内部的维护方式和分类方式。它们是存在于一个安全的、物理及联网访问都得到紧密监控的环境中，还是存在于一个未知的服务器中或者一个甚至很易于入侵的物理文件系统中?

其次，组织机构是否建立了有效的业务控制、政策、体系结构、流程和技术，能够保护、监控和审计由适当的个人对这些数据的访问和使用？这样的保护是否仍然能够允许为合法的业务目的进行便利的访问?

第三，在具有一定监管的、希冀保护个人信息安全性的业务环境中，组织机构是否能够表现出其遵守这些规则？是否保有一定的灵活性，能够适应持续的监管变化?

建立更安全的社交习惯

2011年9月发表的一份Ponemon研究所报告指出，只有35%的被调查者制定了书面的社交媒体策略；这其中只有35%能够积极落实其策略。[7] 遗憾的是，尚没有一套软件或一套端点安全性产品能够很方便地加以部署，以防范社交工程攻击中的诸多类型和方法。就像对付多数以人类为目标的威胁一样，管理此类危险的最佳方法是策略和培训。

特别是，当最终用户使用与工作相关的设备访问社交媒体时，最终用户应当承担的责任包括：

- 启用安全性及隐私性设置。重要的是，最终用户应当了解在他们经常使用的社交网站上有哪些安全性及隐私性控制措施，即使他们不认为自己属于活动用户。为了减少对垃圾邮件、欺诈及伺机攻击者的暴露，他们的安全性及隐私性控制措施应当被设置为最高级别。
- 注意朋友的朋友。如果社交工程攻击不是在某些方面比较聪明，他们就不会如此成功。正如现实世界中的骗子一样，社交媒体攻击者总是从力图获得其攻击目标的某种程度的信任入手。例如，通过Linkedin假冒某种相近的工作关系，往往立即给攻击者带来可信度。最终用户应当谨慎考虑建立友谊的请求，并根据先前的实际工作关系或者可以证明的联系接受此类请求。还应当提请用户注意其关系的下游影响。信任某个人的其他人可能会想当然地假定，他们也可以信任与该人建立了某种关系的任何人。

- 在使用链接和下载时要小心。自从1990年代末期电子邮件无处不在以来，链接和下载就一直是攻击者向其目标传递恶意软件的最得力途经。这种趋势现在演变并扩展至社交媒体领域。最终用户必须极尽谨慎，在点击任何链接或下载任何东西(尤其是可执行文件)之前必须仔细考虑其来源以及适宜性或关联性。可信赖的社交媒体联系人本身可能已经成为受害人，因此，以任何方式与第三方内容打交道时必须多留一个心眼。
- 提防竞赛、礼品、奖品和特价。奖品以及其他特价骗局可以追溯至电子邮件的早期，但其在社交媒体领域的表现依然很抢眼。骗子通常利用此类优惠把最终用户吸引至某个断头网站(dead-end website)，它可能会加载cookies或者甚至是恶意软件，更经常的是，假冒或模仿合法企业或品牌的网站。无论采用哪种方法，骗子总是要从其目标那里收集个人信息。
- 对披露与工作相关的信息要保持谨慎。当最终用户在社交媒体中交流有关其目前参与的组织机构、同事、客户、产品、服务及项目的信息时，一定要咨询其雇主相关的使用政策。如果没有书面的公司政策，就必须遵守企业关于发布与工作相关的信息时的指南。帖子内容应当得到仔细斟酌，因为他们立时就会公开，而且无法收回的。

移动性、社交媒体以及web商务非常清楚地强化了一些重要观念，它们正在重塑组织机构在当今商业环境中开展竞争的方式。因此，更全面地管理它们变得非常重要。

获取完整场景

2011年X-Force报告强调了采取完整方法处理网络安全性的重要性，这种方法既要解决业务挑战，也要解决技术问题。对于繁忙的高级管理人员而言，安全性不是一个简单的能够委托给别人的问题；在日益复杂且由技术推动的世界中，处理安全性问题必须像处理任何业务规划中的其他重要元素一样严肃认真。

随着移动能力和社交能力持续提高，企业需要采用一种统一的方法来预测、识别及预防对个人及其代表的机构发起的攻击。在预测性分析能力、统一的端点管理、数据保护以及社交指南方面的做好准备，将有助于组织机构管理潜在的网络风险。

要想尽早获得IBM商业价值研究院提供的最新深刻洞察，请订阅我们的电子新闻月刊IdeaWatch。地址为：ibm.com/gbs/ideawatch/subscribe

通过从你的应用商店中下载面向iPad或Android的免费“IBM IBV”应用，可以在你的平板电脑上访问IBM商业价值研究院执行报告。

关于作者

Jack Danahy。IBM安全性系统分部负责高级安全性的总监，也是关于软件、系统及数据安全性话题的国际发言人和者。他的联系方式是：*jack.danahy@us.ibm.com*

John Lainhart。IBM全球企业咨询服务部全球安全性及隐私服务领域的领袖，也是美国公共部门网络安全性及隐私服务领域的领袖。他的联系方式是：*john.w.lainhart@us.ibm.com*。

Eric Lesser，IBM商业价值研究院的研究总监和北美领导人。他的联系方式是：*elesser@us.ibm.com*

作者感谢IBM X-Force团队的持续工作和贡献，其中包括Jason Kravitz、Tom Cross、Leslie Horacek、Ralf Iffert、Paul Sabanal、Scott Moore、David Merriell、Mike Montecillo、 Michael Applebaum和Kimberly Madia，他们完成了本文所引用的“2011年IBM X-Force趋势及风险”报告中的内容。

IBM X-Force世界上最著名的商业性安全研究机构之一。有关详细信息，请访问：ibm.com/security/xforce

参考资料

1 “Leading Through Connections: Insights from the Global Chief Executive Officer Study.”IBM Institute for Business Value. May 2012. www.ibm.com/ceostudy2012

2 This executive report is based on data collected in the 2011 IBM X-Force Trend & Risk report. Register to download the latest version at https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=xforce-trend-risk-report

3 The Open Web Applicaation Security Project.“SQL Injection.”December 6, 2011. www.owasp.org/index.php/SQL_Injection

4 Perlroth, Nicole.“Widespread Virus Proves Macs Are No Longer Safe From Hackers.”Bits. *The New York Times*. April 6, 2012.http://bits.blogs.nytimes.com/2012/04/06/widespread-computer-virus-indicates-mac-users-no-longer-safe/?scp=1&sq=macdefender.com&st=cse

5 Press release.“It’s a Social World Report: Social Networking Leads as Top Online Activity Globally, Accounting for 1 in Every 5 Online Minutes.”comScore. December 21, 2011. www.comscore.com/Press_Events/Press_Releases/2011/12/Social_Networking_Leads_as_Top_Online_Activity_Globally

6 Verizon.“The 2011 Data Breach Investigations Report: A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit.”2011. www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

7 Ponemon Institute.“Global Survey on Social Media Risks.”September 2011. www.websense.com/content/ponemon-institute-research-report-2012.aspx

选对合作伙伴，驾驭多变的世界

IBM全球企业咨询服务部积极与客户协作，为客户提供持续的业务洞察、先进的调研方法和技术，帮助他们在瞬息万变的商业环境中获得竞争优势。从整合方法、业务设计到执行，我们帮助客户化战略为行动。凭借我们在17个行业中的专业知识和在170多个国家开展业务的全球能力，我们能够帮助客户预测变革并抓住市场机遇实现盈利。

北京总公司

北京朝阳区北四环中路27号
盘古大观写字楼25层
邮编：100101
电话：(010)63618888
传真：(010)63618555

上海分公司

上海浦东新区张江高科技园区
科苑路399号10号楼6-10层
邮政编码：201203
电话：(021)60922288
传真：(021)60922277

广州分公司

广州天河区珠江新城
花城大道85号
高德置地广场A座9层
邮政编码：510623
电话：(020)85113828
传真：(020)87550182

GBE03502-CNZH-00