

# 从网络钓鱼到高级持续性威胁：企业风险管理模式的风险

非官方中文译本 · 安天实验室 译注

文档信息			
原文名称	From Phishing To Advanced Persistent Threats: The Application Of Cybercrime Risk To The Enterprise Risk Management Model		
原文作者	John W. Moore	原文发布日期	2010 年第 4 季度
作者简介	弗吉尼亚州立大学是美国一所历史悠久的公立 HBCU 政府拨给土地的大学，始建于 1882 年。 <a href="http://en.wikipedia.org/wiki/Virginia_State_University">http://en.wikipedia.org/wiki/Virginia_State_University</a>		
原文发布单位	弗吉尼亚州立大学		
原文出处	<a href="http://www.cluteinstitute.com/ojs/index.php/RBIS/article/view/358/347">http://www.cluteinstitute.com/ojs/index.php/RBIS/article/view/358/347</a>		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
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>		

--	--

# 从网络钓鱼到高级持续性威胁： 企业风险管理模式的风险

美国弗吉尼亚州立大学，John W. Moore

## 摘要

本文探讨了风险环境下存在的各种网络犯罪问题，着重分析美国公众公司广泛使用的衡量财务报告的内部控制框架；同时，还探讨了身份窃取的市场，查看来自这些被窃取身份的资源；本文回顾了可用的内部控制框架并解释了依据《萨班斯法案》第 404 节规定，如何将某公司面临的网络犯罪风险归类为重大漏洞。本文模拟了如何借助 COSO 企业风险管理模式提升组织安全性，避免严重事故发生。

关键词：网络犯罪；内部控制框架；《萨班斯奥克斯利法案》404 节；重大漏洞

## 引言

网络犯罪的目标通常是那些因为考虑到名誉损失和潜在客户流失不会向媒体透露受到攻击的组织。基于网络犯罪的类型及其成功的概率，许多事件将永远不会被揭露。然而，如果成功犯罪的目的是窃取客户姓名、社保号、地址、账户信息及证书，那么这些记录会被转卖给犯罪团伙以供身份窃取。随后，这些信息将毫无悬念的被公诸于众。身份窃取不是网络犯罪的唯一目标，但却是公众最熟知的目标。

作为在美国发展最快的网络犯罪形式，身份窃取已经获得公众和媒体的广泛关注，迫使制订州和联邦级别的立法，阻碍数百（可能数千）起公众交易和私人业务、非营利组织、教育机构和政府机构等。愤怒的消费者花费大量时间和金钱试图理顺受损的信用记录，并解决那些他们根本不应承担的账单。但某个组织包含其客户、捐赠者、学生、员工、退伍军人、纳税人或是病人的 PIN 丢失或被盗时，就会出现严重的法律、财务和名誉后果。很快，失去客户的信任、名誉的损失及某个组织品牌的受损会接踵而至。花费金钱修复这些损失会相当昂贵。对于上市的公司，其股价也会下跌（Rapoport, 2005）。

我们所听说的关于身份窃取的案例分为两大类——钓鱼攻击和数据泄露。钓鱼攻击通常的策略是，假冒金融机构，发送大量的垃圾邮件，声称用户账户出现了急需解决的问题。Synovate (2007)表示大约有 5% 的用户会相信这些信息并点击邮件中附带的链接。他们被定向到一个看似是他们所查询金融机构实则虚假的站点。一旦他们输入个人信息，窃贼将成功的搜集大部分可能全部的用于窃取网络身份的信息。数据泄露可能暴露存储在某组织数据库内数百万的信息记录，其目标通常为掌握大量记录的组织。这两种事件都能导致 PII 丢失，PII 被有组织的犯罪团伙频繁的用于网上交易。这两类事件的相同之处在于，钓鱼攻击针对的是某家公司，窃取其客户身份，可能导致客户相信这是该公司的责任，尽管应该归咎于虚假的网站；数据泄露不会导致数千或数百万的记录暴露，通常针对的也是某个特殊的公司，尤其是被泄露的信息足够多时，会遭到公开披露。不管哪种情况，公司都无法逃脱被指责的境地。

本文包括以下章节：事件性质、数据泄露和身份窃取的程度及相关成本的描述；美国上市公司使用的内部控制框架的探讨；企业风险管理模式对网络风险的应用；结论及对未来工作的建议。

## 数据泄露和身份欺诈范围及程度的信标

身份窃取不是互联网的产物 ( Peretti, 2009 )。这是一种古老的犯罪模式,通过技术的运用使其更加有效和有利可图。互联网所做的只是使有组织的地下市场的形成成为可能,互联网聊天室和论坛,用于交易窃取的身份信息并分发将 PII 换成现金所需的产品和服务。互联网计算机安全产品提供商赛门铁克,记录了这种“服务器经济。”2009 年,最具标榜性的数字身份报价为:信用卡信息是 85 分到 30 美元不等,占据宣传的 19%;银行账户证书为 15 美元到 850 美元不等,也占 19% ( Symantec, 2010 )。这种服务器经济使非法交易大量的 PII 成为可能。

如表 1 所示 身份窃取事件发生的概率在 2007 年下滑,但在 2008 和 2009 年又开始回升( Javelin Research and Strategy, 2007, 2008, 2009, 2010 )。表中显示的金额为实际盗取金额,不包括消费者解决事情的花费。很多情况下,蒙受损失的是银行和其他机构,因此这表示在互联网上经营业务成本的增加。

表1： 美国身份窃取导致的大约损失

年份	身份窃取案件数量	导致的损失
2006	840万起	493亿美元
2007	810万起	450亿美元
2008	990万起	480亿美元
2009	1110万起	540亿美元

在服务器经济产业,窃取的身份非常有价值,因此有组织的犯罪团伙将掌握大量PII数据库作为目标也就不足为奇。每年一度的《Verizon数据泄露调查报告》(2010, 2009)描述了他们为客户调查每年泄露的信息的细节。表2中,2008和2009年的数字显示了Verizon和美国特勤局联合处理的事件总量(都是金融欺诈诉讼事件)。应注意,2009年每起数据泄露事件暴露的平均记录值都超过了100万。

表2： 2007至2009年记录信息泄露事件数量

年份	信息泄露事件数量	入侵次数
2007	171,077,984	128
2008	360,834,871	192
2009	143,643,022	141

当数据泄露事件的负责人可以明确确定的情况下,最大的犯罪者则是来自组织外部的资源。令人不安的是,45%由黑客攻击导致数据泄露事件中,计算机系统的防御措施都被成功渗透。然而,这些事件占据表3中记录的96%。

表3： 信息泄露负责方分布 (2009年)

负责方	外部资源负责	内部人员负责	合 作 伙	多代理人
事件数量	138,566,355	2,640,240	130	2,436,297
百分比	45%	27%	1%	27%

组织遭遇数据泄露要蒙受巨大的损失。2009 年,在针对 45 家遭遇数据入侵的组织调查发现,它们在这方面的平均损失为 675 万美元,大致的损失范围为 75 万至 3100 万美元 ( Ponemon, 2010 )。股市估值损失为另一个方面。在针对 1996 年至 2001 年间发布遭遇恶意(并非偶然)互联网安全入侵的 66 家公众公司的

调查中发现,遭遇入侵 2 天后,该公司的股市估值平均下降 2.1%,或每起入侵事件损失 16.5 亿美元(Cavsoglu, Mishra, and Raghunathan, 2004)。

与身份窃取从个人犯罪发展成有组织的犯罪一样,公司遭遇网络犯罪事件的风险也在不断发展,从个人到组织运营间谍活动活和 APT 攻击,APT 极具针对性和风险性,目标为某个公司或产业。可以用某个术语描述组织信息系统遭遇入侵,可以是未曝光的和持续数月的。这就给攻击者挖掘大量数据提供了时间,近期的案例为 2010 年针对谷歌、银行、国防承包商、化工制造商及政府机构的攻击(McDonald, 2010)。APT 攻击的目标看似获取 R&D 信息、军事机密或是另一个国家的经济利益信息(国防部长办公室, 2010)。Geer (2010) 将 APT 定义为“用难以被发现、清除和定性的手法获取或改变信息的努力尝试。”需要关注 APT 的以下三方面:第一,其目标为数据,由于它只是简单的拷贝,所以信息所有者很长时间都不会意识到自己的损失;第二,用户频繁地点击某个链接将允许攻击软件访问公司的信息系统;第三,软件可进行自我改变和加密,以降低被检出的可能性(Cole, 2010)。

考虑到网络犯罪的程度及相关的损失风险,它似乎适合那些面向互联网的组织将这些风险纳入到自身的风险评估程序。虽然适用于大多数组织,但它更适用于那些《萨班斯法案》授权内部控制的公司。接下来的部分将回顾在美国证券交易委员会监管文件里最频繁提到的内部控制框架。

### 评估财务报告的内部控制的框架

2002 年《萨班斯法案》的通过引起最具争议的问题可能是美国证券交易委员会注册人针对金融报告的内部控制的有效性的管理评估和审核认证。作为管理报告的部分内容,法案必须命名用于评估内部控制系统的组织框架。

虽有国际上存在很多可用的框架,但本文专注于那些在美国监管机构备案最常提到的内容:

- Control Objectives for Information and Related Technology (COBIT, 2005)
- COSO's Internal Control – Integrated Framework (1992)
- COSO's Enterprise Risk Management – Integrated Framework (2004)
- COSO's Guidance for Smaller Public Companies (2006)

为达到评估内部控制系统的多个目的,SEC 需要借助于有组织的控制框架和 PCAOB 审计标准 5 号文件。“内部控制对财务报告已整合的财务报表进行审核”要求审核员使用与管理评估相同的框架。Compliance Week 的研究显示,数千家上市公司使用 1992 框架。这明显小于使用企业风险管理框架的数字,同时也小于使用 1992 框架和 COBIT 模式结合的数字。数百家公司报道称使用《小规模上市公司指南》。许多公司已经开发或购买企业的风险管理系统。

这些框架作为某家公司评估其控制策略和规程的基准。具体内容如下:

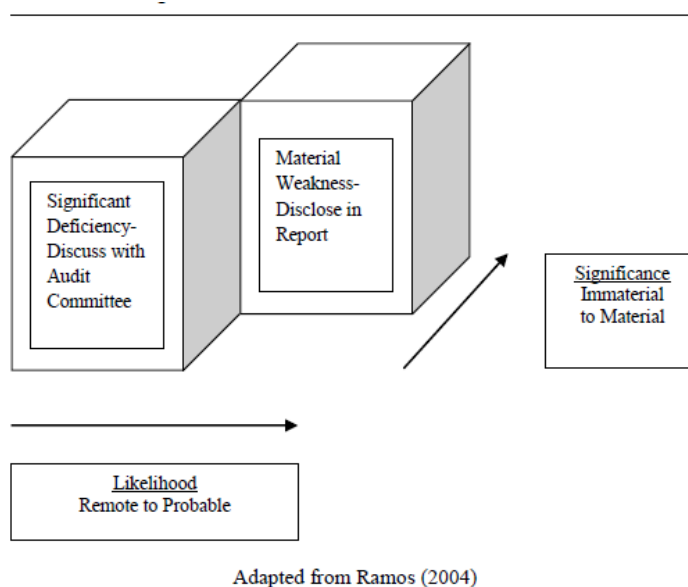
- Control Objectives for Information and Related Technology (COBIT)。由于信息技术控制指南,很多组织依赖 COBIT 框架。COBIT 是 ISACA 的一个产物(信息系统审计与控制协会),它的首次发布是在 1996 年,2005 年发布了第四个版本。COBIT 涉及 IT 系统和相关技术的生命周期控制。基于这一点,一些上市公司使用经过 COBIT 补充的 1992 COSO 指南。

- COSO's Internal Control – Integrated Framework。Treadway委员会发起人组织 (COSO) 颁布有关内部控制的第一个指南,为会计和审计委员会的内部控制设计提供一些统一性。上市公司广泛应用这一框架。该框架从管理的角度聚焦内部控制,不具有风险管理的相关特性。
- COSO's Enterprise Risk Management – Integrated Framework。2004年, COSO发布企业风险管理—整合框架以扩展内部控制并提供企业级风险管理的视角。
- COSO's Internal Control over Financial Reporting – Guidance for Smaller Public Companies (2006)。该指南没有修改原始的1992框架,但其目的在于帮助小型公司以成本效益设计、实现并维持内部控制。其中包含一套说明性评估工具。

《萨班斯法案》奏效的 6 年后,这些指南仍就被需要。举例说明, Compliance Week 对 2010 年上半年的研究揭示了 290 家公司报道无效内部控制而导致财务报告中一个甚至多个重要漏洞。

2002 年《萨班斯法案》第 302 节,要求上市公司管理层证明内部控制对财务报告的充分性。第 404 节要求公司审计员证明并报告管理层对内部控制的评估。302 节规定,管理层负责建立、维持并定期评估其针对金融报告的内部控制的有效性。如果发现漏洞,必须从重要性和相似性两方面进行评估,以确定它们的相对重要性 (见图 1)。这种对内部控制漏洞的评估必须考虑到内部控制系统是否能够阻止财务报表出现重大错误。这就要考虑到发生的相似性 (从低到高) 和潜在错误的重要性 (从无到有)。如图 1 所示,如果那些看似不可能发生的情况被判定为重要的,那么他们会在舆论的指导下被披露。那些不会上升到重大漏洞级别的重要漏洞将不会被报道,但需要与审计委员会进行探讨。

图 1：内部控制漏洞展示



### 网络犯罪风险在 ERM 框架下的应用

在美国,企业风险管理并没有向其他地方那样被广泛采用。比斯利,布兰森和汉考克 (2010) 报道

“全球 46%的受访者将他们的风险监督过程描述成系统的、健全的和可重复的。相比之下,11%的美国受访者认为他们已经有一套完善的企业风险管理流程落实到位。( p. 4 )”

他们发现的结果本文予以证明。之前提到大部分公司看似还在使用原始的 COSO 框架，不断的由公司被迫报道他们的 ICFR 是无效的。如果有公司无效的 ICFR 使用最古老的框架，那么必须考虑是否有额外的未被监测到的风险。升级他们的框架至企业风险管理模式，将通过评估公司的风险和机遇，提升价值。以下为 COSO ERM 模式的简介，后续文字对其如何实现进行详细地解释说明。

2004 年，COSO 发布 ERM（企业风险管理——整合框架），将之前的内部控制焦点结合风险管理：

“EMR 是一个过程，受一个机构董事会、管理层和其他部门的影响。使用战略设置遍布整个企业，设计的目的在于识别影响机构的潜在事件，并管理内部风险，为企业目标实现提供合理保障。”（COSO, 2004）

只要风险可理解回报可接受，那么这种方法就允许管理人员利用这些机遇。

COSO 框架为企业识别潜在的风险、评估特殊风险的影响及发现管理风险的方式提供最全面的工具。该文档提供以下四个类别助力企业实现目标：

1. 战略——高层次目标，与其使命一致并加以支持。
2. 经营——有效并充分利用资源。
3. 报告——报告的可靠性。
4. 合规——遵守适用的法律法规。

企业风险管理，由 COSO 设想并提出，是一家公司运行方式的产物。作为理解风险的结构，应考虑到 8 个内外部的代理和事件（见表 4）。在合并网络犯罪风险的风险管理计划的背景下，COSO 设想的 ERM 模式为应对这些风险做好了准备。三个相关的部分（阴影部分）为事件识别、风险管理和风险响应。

**表4：COSO ERM 内部控制组成**

组成成分	描述
内部环境	<ul style="list-style-type: none"> <li>• 组织基调</li> <li>• 风险管理哲学</li> <li>• 风险偏好</li> <li>• 董事会</li> <li>• 诚信、道德价值观和能力</li> <li>• 组织结构</li> <li>• 权力和责任分配</li> <li>• 人力资源标准</li> </ul>
目标设置	<ul style="list-style-type: none"> <li>• 战略目标</li> <li>• 经营目标</li> <li>• 报告目标</li> <li>• 合规目标</li> </ul>
事件识别	<ul style="list-style-type: none"> <li>• 影响战略实施或目标实现的事件</li> <li>• 外部因素 – 经济、自然环境、政治、社会和技术</li> <li>• 内部因素 – 基础设施、人员、流程和技术</li> <li>• 识别技术</li> </ul>

风险评估	<ul style="list-style-type: none"> <li>• 固有和剩余风险</li> <li>• 估计相似性和影响</li> <li>• 评估技术</li> </ul>
风险响应	<ul style="list-style-type: none"> <li>• 响应选择：规避、降低、分担和接受</li> <li>• 组合观察</li> </ul>
控制活动	<ul style="list-style-type: none"> <li>• 有关战略、经营、报告和合规性目标</li> <li>• 结合风险响应</li> <li>• 控制活动类型</li> <li>• 政策和规程</li> </ul>
信息和通信	<ul style="list-style-type: none"> <li>• 系统结合外部资源</li> <li>• 技术选择影响目标实现</li> <li>• 依赖系统实现战略和经营目标，减少安全入侵和网络犯罪风险</li> <li>• 通信：内部和外部</li> </ul>
监控	<ul style="list-style-type: none"> <li>• 持续监控活动</li> <li>• 独立评估</li> </ul>

### 事件识别过程

COSO 提出五大“事件类别”作为识别威胁和机遇的出发点：经济、自然环境、政治、社会和技术。如表 5 所示，像钓鱼攻击和数据泄露这类网络犯罪，可能影响组织除了自然灾害以外的所有类别。至于剩下的四个事件类别，有一个或多个对组织构成威胁的外部因素。表示威胁存在的风险包含在威胁内。

表 5：外部因素和身份盗窃风险

事件分类	外部因素	威胁和风险案例
社会	隐私； 消费者 行为；  恐怖主义； 服务器经济	定向钓鱼攻击导致用户个人信息被贩卖给犯罪分子，供其用于身份窃取： <ul style="list-style-type: none"> <li>• 诉讼，损害赔偿</li> <li>• 用户损失</li> <li>• 负面宣传</li> <li>• 公示法律可能要求披露</li> </ul> 有组织的犯罪团伙执行大规模的行动窃取用户身份信息，导致数据泄露： <ul style="list-style-type: none"> <li>• 诉讼，损害赔偿</li> <li>• 用户损失</li> <li>• 负面宣传</li> <li>• 公示法律可能要求披露</li> <li>• 可能被迫长期向外部安全审计提交</li> </ul> 存在有组织的市场贩卖身份数据： <ul style="list-style-type: none"> <li>• 对窃取的个人数据需要的增长</li> <li>• 目标可以是任何存在大漏洞的网站或计算机</li> </ul>



技术	电子商务       新兴技术	如果只有在线业务，那么业务模式暴露在风险中。 • 电子商务的所有部分都在服务器上。 • 用户、捐赠者或其他利益相关者的身份窃取。 • 货币/货物的窃取。 • 被攻击的用户列表。 引进的新技术弥补了原有内部控制的不足。 • 无线网络 • 会话中弹出窗口 • APT
经济	企业并购   合作伙伴   外包	对目标/合作伙伴信息系统内部控制的调查。 • 对合作伙伴敏感个人信息清单缺乏了解。 • 缺乏对合作伙伴访问/使用你的账户的政策和控制。 • 国外厂商难以起诉。 • 需要SAS 70数据中心审计。 • 厂商缺乏控制。
政治	立法； 法规； 公共政策	州和联邦立法机构将制定严格或昂贵的条款。 • 扩展到一个新的国家/民族审查现有的控制，以符合该机构的规则。

### 风险评估过程

从表 5 中事件清单可以过渡到下一个内容—风险评估。这里我们考虑固有风险和剩余风险。固有风险是指管理层不采取措施限制的情况下存在的风险总量。余下风险演变成剩余风险。表 6 是评估某些特定事件是否会导致身份窃取发生和发生事件可能性的假设案例。COSO 提出在未来的 18 个月内，某个时间框架可能被设置。这就有助于将分析限制在短期内，也是建立周期性练习而不是一次性事件的方法。

表6：对身份窃取的风险评估

描述项	发生的可能性	风
可能	中等	钓鱼攻击导致用户身份被窃取
不会	低	数据泄露倒是用户身份被窃取
很可能	高	新的立法将要求经过修订的或新的内部控制
可能	中等	无线网络将被与差的空间一起安装

### 风险响应过程

一旦风险评估完成，管理层便可以考虑应对这些风险的方法。在 COSO 模式下，有四种选择——规避、降低、分担和接受。表 7 给出每一个类别中组织应考虑身份窃取或其他形式网络犯罪的可能性。

表7：对身份窃取可能的风险响应

风险规避	风险降低
------	------

<ul style="list-style-type: none"> <li>• 重新设计信息避免被收集</li> <li>• 停止/出售需要个人数据的业务线</li> </ul>	<p>网站</p> <ul style="list-style-type: none"> <li>• 与监控服务的网站签订合同</li> <li>• 购买相似的域名</li> <li>• 以安全厂商身份注册网站</li> <li>• 与域名托管服务签订合同</li> </ul> <p>数据清单</p> <ul style="list-style-type: none"> <li>• 查看数据保留策略</li> <li>• 创建数据销毁时间表</li> <li>• 敏感数据存储位置清单</li> <li>• 旧的存储媒介的销售策略</li> </ul> <p>管理</p> <ul style="list-style-type: none"> <li>• 应急计划</li> <li>• 管理用户密码更改</li> <li>• 负责人</li> </ul> <p>厂商、员工</p> <ul style="list-style-type: none"> <li>• 查看与数据经纪人的关系</li> <li>• 供应商对安全性的审核，数据中心的审核</li> <li>• 背景检查</li> </ul>
风险分担	风险接受
<ul style="list-style-type: none"> <li>• 与厂商、用户和合作伙伴签订合同</li> <li>• 外包给美国当地厂商</li> <li>• 购买网络保险</li> </ul>	<ul style="list-style-type: none"> <li>• 接受该公司风险承受范围内的风险</li> <li>• 自保</li> </ul>

## 结论

如果上述描述的一个或更多事件将发生，那么它可能会影响公司的经营及合规目标的实现。

依据事件识别部分，钓鱼攻击和数据泄露是一个常见的问题，应该包含在对公司构成风险的事件内。如果被认定为是一个导致风险的事件，那么就需要进行合理的风险评估和风险响应。

网络钓鱼和其他形式的电子攻击显然对经营及合规性目标产生不利影响。经营目标，如盈利能力，可能受到抵抗和关闭钓鱼网站支出成本的影响。由于钓鱼攻击通过劫持知名和可信的品牌实现，那么保护资源/资产，包括品牌本身在内，都将受到攻击。

当在线身份被盗时，隐私保护始终是一个问题。如果有足够的记录被攻破，攻击可能导致这一事实的公示（这取决于该公司位于哪个州）。电子形式的恐怖主义可以是针对一家公司、政府机构或互联网服务提供商简单的 DoS 攻击。

专有数据的损失，如营销计划、研发工作、并购调查报告或者其他对组织有价值的信息，可能导致公司的信息系统遭遇攻击。蒙受这类信息损失的公司没有意识到外部资源已在它们的系统里植入了软件，有时这种情况可持续很长时间。随着时间的推移，会有更多宝贵的数据丢失。

技术风险包括电子商务和新兴技术的风险。一旦一家公司开设了网站，那么它将面临全球的威胁。越来越依赖网站（如销售份额），将使公司暴露在这些风险中。新兴技术可能代表一种新的威胁或者是现有威胁的一个改变。例如，当用户进行一次网银会话时，会弹出钓鱼窗口。在这种颇具针对性的攻击中（该银

行所有的用户都遭遇欺骗), 会弹出一个窗口, 提示用户会话超时, 需重新输入用户名和密码。一旦犯罪分子获取用户名和密码, 用户便会重新回到真正的银行网站。

Ge 和 McVay (2005)提出了重大漏洞分类的计划, 共包含九种类型的漏洞。以下五种类型的漏洞可与网络犯罪风险关联到一起:

- 高级管理人员 ( 允许无效的内部控制环境 ): 一个不熟悉网络威胁的管理团队不能理解什么时候需要额外的资源, 如更有经验的人员或安全监控公司。
- 培训 ( 培训或人员配备不足, 导致无法有效并及时执行评估 ): 大量钓鱼攻击和数据泄露事件可以数周甚至数月不被检测到, 这是因为没有及时做好计算机安全的评估以至于无法检测到问题的存在。这方面的例子不包括读取系统日志检测未授权软件的安装, 也不包括测试从系统发出异常数量的数据。
- 技术问题 ( 对于电子商务, 所有内容都位于服务器上 ): 用户担心其 PII 的安全, 同时也担忧 DoS 攻击削弱业务能力, 导致经营问题不断出现。
- 特殊账户: 任何可能需要偿还消费者的损失或提供信用卡监控服务的身份窃取, 都代表一种未来的责任, 因此这种责任将被低估。
- 特殊账户 ( 可能导致知识产权损失的攻击 ): 如果资产被购买, 那么可能出现减值的问题; 在这种情况下, 资产在财务报表中会被高估。
- 账户策略: ( 缺乏对合作伙伴使用的组织信息资产的控制 ): 商业合作伙伴或合同商对信息的控制可能导致数据损失或挪用。

### 对未来研究的建议

随着网络犯罪的发展, 更多的公司成为受害者, 这可能导致 ERM 被广泛采用。如果政府和大型上市公司继续遭遇 APT 攻击, 这就可能驱使更多的公司将这些威胁纳入到它们的风险评估中。下面内容是给未来研究的建议。基于报道漏洞的类型和数量, 将使用原始的 1992COSO 模式和使用 ERM 模式的公司进行的对比, 可以从识别产业和属性的角度指导采用 ERM。在安全性方面, 信息安全预算的对比可能导致模式预算; 信息安全功能外包情况的评估可能导致更好地理解那些有用和无用的信息。

## 参考文献

1. Beasley, Mark S., Branson, Bruce C. and Hancock, Bonnie V., 2010. Enterprise risk oversight A global analysis. CIMA and AICPA research series. The ERM Initiative at North Carolina State University, [www.erm.ncsu.edu](http://www.erm.ncsu.edu)
2. Cavsoglu, Huseyin, Mishra, Birendra, and Raghunathan, Srinivasan, 2004. The Effect of Internet Security Breach on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, Fall 2004, Vol. 9, No. 1, pp. 69-104.
3. Cole, Eric. 2010. Advanced Persistent Threat (APT). McAfee Security Insights Blog. <http://siblog.mcafee.com/cto/advanced-persistent-threat-apt/>
4. Committee of Sponsoring Organizations, 2004. Enterprise Risk Management-Integrated Framework, Executive Summary. New York: The Committee of Sponsoring Organizations of the TreadwayCommission, 2004.
5. 2006. Internal Control over Financial Reporting – Guidance for Smaller Public Companies. New York: The Committee of Sponsoring Organizations of the Treadway Commission, 2006.
6. Ge, Weili and McVay, Sarah. 2005. The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. *Accounting Horizons* 19(3): 137-158.
7. Geer, Daniel. 2010. Advanced Persistent Threat. *Network World* April 12, 2010. <http://www.networkworld.com/news/tech/2010/041210-tech-update.html>
8. Javelin Research and Strategy. 2007. <http://www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study>.
9. Mills, Elinor, 2009. Payment Processor Heartland reports breach. Cnet news, January 20, 2009. [http://news.cnet.com/8301-1009\\_3-10146275-83.htm](http://news.cnet.com/8301-1009_3-10146275-83.htm)
10. McDonald, Joe, 2010. Google charge highlights China-based hacking. Msnbc.com, Feb. 3, 2010. [http://www.msnbc.msn.com/id/35222681/ns/technology\\_and\\_science-security](http://www.msnbc.msn.com/id/35222681/ns/technology_and_science-security).
11. Office of the Secretary of Defense, 2010. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. [www.defense.gov/pubs/pdfs/2010\\_CMPR\\_Final.pdf](http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf)
12. Peretti, Kimberly Kiefer. 2009. Data Breaches: What the Underground World of “Carding” Reveals. *Santa Clara Computer & High Tech Learning Journal*. Vol. 25, pp376-413.
13. Ponemon Institute LLC, 2010. 2009 Annual Study: Cost of a Data Breach. [www.ponemon.org/localupload/fckjail/generalcontent/18/file/US\\_Ponemon\\_CODB\\_09\\_012209\\_sec.pdf](http://www.ponemon.org/localupload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf)
14. Ramos, Michael, 2004. Section 404 Compliance in the Annual Report. *Journal of Accountancy*. New York: Oct. 2004. Vol. 198, Issue 4, pp 43-47.
15. Rapoport, Michael, 2005. Companies Pay a Price For Security Breaches; In Most Cases, Shares Fall Moderately After Disclosure And Then Can Stay Down. *Wall Street Journal* (eastern Edition) June 15, 2005: (C3).
16. Symantec Corporation. 2010. Symantec Global Internet Security Threat Report – Trends for 2009. Vol. XV, April 2010.
17. Synovate, 2007. Federal Trade Commission – 2006 Identity Theft Survey Report. <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.
18. Verizon Business. 2009. 2009 Data Breach Investigations Report. [http://www.verizonbusiness.com/resources/security/reports/2009\\_databreaches\\_rp.pdf](http://www.verizonbusiness.com/resources/security/reports/2009_databreaches_rp.pdf)
19. Verizon Business. 2010. 2010 Data Breach Investigations Report. [http://www.verizonbusiness.com/resources/reports/rp\\_2010-data-breach-report\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf)