09 年安全走向预测

09 年安全走向预测

2009 年的安全形势与经济危机虽然没有直接关系，但是也会受到影响，例如企业的合并、安全预算的缩减、裁员、安全设备的选择等等，那么在新年中，安全形势将会发生哪些变化呢？在本专题中，TechTarget 中国的安全专家将会与大家共享对未来的 IT 安全形势的看法。

网络安全

全球经济和业务蓝图的变化很可能将不会对信息安全产业产生很大的影响，但是企业的合并和安全预算的缩减已经成为必然，因此在 2009 年企业需要考虑如何用更好的钱做更多的事儿，而安全厂商的壮大与否也会影响企业的选择……

- ❖ **网络安全 2009 趋势：合并与安全预算缩减**

Web 威胁

2008 年 Web 病毒数量增长迅猛，严重威胁企业 IT 安全。2009 年 Web 威胁将会呈现什么样的趋势，企业应该如何应对？趋势科技的产品技术顾问认为 2009 年的 Web 病毒数量仍然呈上升趋势。

- ❖ **专访趋势科技：Web 威胁将持续增长**

数据泄露

管理顾问 KPMG LLP 最新的报告显示，受到信用危机的影响，个人和金融数据的丢失在 2009 年将会急剧上升。基于目前的形势，KPMG 说随着信用危机的加深，全球受到数据丢失影响的人数将在 2009 年增长到 1.9 亿，而在去年是 0.92 亿。

❖ KPMG：数据泄露将呈上升趋势

企业攻击

本部分基于去年的威胁和攻击，对 2009 年的安全信息简单预测。但是今年和不久的将来要面对的新威胁和过去所面对的看起来类似。例如，无线风险将会继续、以及对杀毒产品的关注将会增加……

❖ 未来的安全威胁：2009 年企业攻击

内部威胁

所有行业的公司都已经开始裁员了。可能开始的时候是削减冗员，但是不可避免的有些公司将会裁掉一些优秀的 IT 和信息安全专家。而这些安全人员存在转为黑客的可能，因此网络犯罪也会增加，而犯罪也会更复杂，例如数据窃取和社会工程。虽然很难想象，犯罪活动经常是以前的拥有这类合法操作的员工所造成的。随着世界经济的混乱的状态、市场的自我修复和裁员，违法的内部活动较之前更加强大，认证和访问管理专家在 2009 年将会面临什么挑战呢？

❖ 2009 认证和访问管理：裁员和内部威胁

预算削减对策

由于经济状况的影响，很多安全经理被要求缩减预算。在本专题中也有多处提到安全个方面预算的削减，那么应该如何应对这种情况，保障企业的 IT 安全呢？

❖ 经济困难时如何保障安全预算？

网络安全2009趋势：合并与安全预算缩减

在新年的时候停下，并思考一下下一年将会出现的安全趋势，是很有趣很有价值的事情。全球经济的变化和业务蓝图很可能将不会对信息安全产业产生很大的影响。我们具体看一下网络安全的预测，以及企业为这些可能性作了什么准备。

用更少的钱做更多的事儿。我承认这不是火箭科学。全球经济正处于艰难时期对任何人来说都不奇怪了，我们甚至已经可以看到一点光亮了。对于还没有被要求减员或者降低预算的安全经理来说，现在是开始起草可能性意外计划的最好时间。虽然希望安全预算保持不变，但是安全经理应该考虑如果出现5%、10%甚至更高的预算缩减，他们应该如何处理。即使预算没有削减，这种训练也很有用，因为这对于目前使用的金融资源的较低的效率起到了启示作用。另外，考虑一下优化安全员工使用的问题。如果计划在不久的将来增加员工，那么就有机会被问到这些不重要的计划。你的员工有没有低投入高产出的方法？如果有可能，员工愿不愿意转为兼职？如果今年预算紧张，灵活的工作安排或者置位的变化是否可以被用于作为增加工资的另一种选择？管理服务提供商（下面将提到）时候可以帮助减少对员工的需求？

保留工作总是首先考虑的，为了这么做，可能很必要证明你看到了底线，并且原因为了公司的利益考虑艰难的选择。例如，如果你今年购买更新了昂贵的防火墙，那么考虑更新周期是不是可以扩展到12个月就很明智。从四年的硬件更新周期到五年的周期就等于20%的成本节省。如果在分析之后，决定更新需要现在就做，就要准备向CIO解释为什么应该首先考虑新的产品而不是其他。

有些厂商可能会关门或者变强。艰难的经济时期不仅限于客户端的我们。我们紧缩的预算会在厂商中产生连锁反应。目前处于“泡沫上”的厂商可能会消失。那些拥有强大的产品和/或客户基础的厂商可能会被想要 扩张的大厂商收购。我已经在2008年底看到了这种事情的发生。如果你们也正处于这种购买的模式种，这是需要记住的一种重要趋势。

买家要在和可能没办法继续生存的小厂商建立长期关系之前三思而后行。厂商的流失对网络安全的操作将产生严重的影响。根据设备的类型和在基础架构中的作用，它可能会严重影响到企业的安全状态。例如，将要倒闭的防火墙厂商就是一个很大的问题。如果设备出现故障或者不能使用等等，就不能获得支持，而这将会危害到整个架构的有效性。这就是说，杀毒厂商的失败是大灾难；病毒定义更新将不会继续，而企业恶意关键防御系统的有效性也会急剧下降。在选择厂商的时候，除了要考虑金融的稳定性的标准，现在也是考查所有目前的厂商的金融状况并决定是否需要重新评估这些关系的最佳时期。

管理服务提供商将继续上升。很多安全服务正在迅速接近日用的状态，而且处于裁员的压力，很多企业都在寻求尽可能的外包安全工作的方法。我们已经看到一些企业采用软件即服务（SaaS）产品，例如 Qualys Inc.的漏洞扫描平台和 WhiteHat Security Inc.的应用漏洞扫描器，作为降低成本的一种方法。同时，传统地销售安全应用的厂商也在向 NOC 的方式转变，提供 24x7 的防火墙监控和维护、入侵防御系统等等。SaaS 安全工具提供了很多的好处。企业不再负责维护和更新产品，而员工就专注在核心的专业技术：安全管理上。管理服务提供商向前走了一步把分析外包了。从不重要的方面来说，使用任何服务都有一定的风险，因为和安全状态相关的机密信息需要和第三方共享。如果你没有考虑使用这些服务，就把它放在你的短期防线上吧。

从法规到操作的转变。不管你喜不喜欢，我们中有很多人都在最近的三五年关注法规问题。PCI DSS、萨班斯法案、HIPAA 和 GLBA 只是安全经理必须管理和帮助的一小部分法律法规。既然这个行业已经关注了一段时间的法规，遵守的紧急性和广泛性就降低了一级。很期待看到企业从安全资源回到支持的工作上的内部压力，可以主动向业务提供安全咨询支持。

我并不想把 2009 年描绘成阴暗无希望的画面；以后的一年将会充满增长和取得显著成绩的机会。抓住这个机会，充分利用人才和金融资源。企业定期重新评估支出、厂商关系和业务的重要性是很健康的行为。但是像鸵鸟一样把头埋进沙子里，企图忽略经济转态和对业务的潜在影响是很无知的。采取机会主义的态度并为我们将会面对的必然寄予做好准备非常重要。

(作者：Mike Chapple　译者：Tina Guo　来源：TechTarget 中国)

专访趋势科技：Web 威胁将持续增长

2008 年 Web 病毒数量增长迅猛，严重威胁企业 IT 安全。2009 年 Web 威胁将会呈现什么样的趋势，企业应该如何应对？在 TechTarget 中国的这次访谈中，趋势科技的产品技术顾问徐学龙先生分享了了他对这些问题的看法，他认为 2009 年的 Web 病毒数量仍然呈上升趋势。

TechTarget 中国：根据趋势科技的统计，Web 威胁从 2005 年到 2008 年三月增长了 1731%。在 2008 年中，您认为哪些 Web 威胁给企业带来最大的安全隐患？

徐学龙：从 2008 年的情况来看，病毒、木马、间谍软件的海量出现对企业的安全生产带来最大的威胁。2008 全年产生的恶意程序总量超过了过去 20 年的总和，而且这些恶意程序大多数都具备自我更新和外窃机密数据的能力，对企业的隐性伤害更大。

TechTarget 中国：您认为在 2009 年 Web 威胁将呈现什么样的趋势？

徐学龙：根据今年病毒的发展特征，我个人认为：基于 Web 病毒的传播技术以及用户对网络应用需求的提升，明年 Web 病毒数量仍然呈上升趋势。

病毒传播途径以及攻击技术都在不断变化，随着网络威胁的涌现，恶意软件已经从爆发模式发展到隐蔽的“睡眠式”感染。1988 年，全球共搜集发现了 1738 例病毒样本，而 2008 年单月搜集的数量就超过了 64 万例（平均一天约 2 万，每隔 4 秒一个病毒）。应对平均每四秒不到就有新病毒产生传播速度，传统的代码比对技术正面临着越来越大的困境。另外，还有一个原因在于，中国用户对于信息化的管理成效已经给予肯定，在未来几年，信息化建设仍然会是中国政府大力推广的重点内容。这也就是说，用户基于 Web 的应用需求也成为病毒数量增长的另一原因。

TechTarget 中国：为什么 Web 威胁的增长速度会这么快？

徐学龙：近 20 年来，网络恶意攻击呈爆炸性增长态势。Web 威胁的增长速度会之所以这么快，我认为与现代科技、防护水平和用户的安全意识密切相关。

首先，每隔 4 秒一个病毒的生成速度与现代科技密不可分，每一项新的技术诞生也会为病毒技术提供发展的平台。

其次，Web 威胁的高速传播也侧面反映出一个问题，那就是传统病毒特征码对比技术的落伍，出现了与病毒对抗的失衡。传统的反病毒技术应付这些 Web 病毒，需要先获到病毒样本，然后进行研制作出解药，再通过兼容性测试，最终还需端点用户下载更新病毒代码才能实现真正的病毒防护工作。仅针对制作病毒特征码的环节，每个病毒样本处理周期就需要 2 小时才能完成，由于病毒仍在持续加速产生，这对任何一个安全厂商来讲，如果没有技术上的革新，最终都会走到一个人力的瓶颈。目前单个病毒的生命周期日益缩短，病毒特征码的防护有效性正变得越来越低，传统的病毒特征码比对技术因此变得性价比越来越低。

最后一个原因在于用户的安全意识问题。应对大量的潜藏性 Web 威胁，用户的安全意识不足也会助涨病毒散播。因此，企业的网络安全，不仅需要强大的技术支持也需要用户本身树立风险意识，加强安全管理。

TechTarget 中国：趋势科技是否将采用新技术应对不断增长的 Web 威胁？

徐学龙：趋势科技认为云安全将是全球领先的反病毒技术。相信，在未来几年，云安全技术仍然是众多安全厂商投资的方向。趋势科技将会继续加大对云安全在人力以及财力方面的持续投入，除了加强云端的计算能力外，强化云安全的服务功能也是未来的主要工作。

目前，趋势科技在全球超过 1000 位安全专家，在全球建立了五个数据中心，拥有数千台云计算服务器和 34000 多台云服务服务器，具有相当高的可靠性。云安全可以支持平均每天 50 亿笔点击查询，99%的用户请求无需重新计算都可以直接在云端得到查询结果。借助云安全，趋势科技现在每天阻断的病毒感染最高达 1000 万次。

趋势科技云安全架构的6大杀手锏（Web信誉技术、邮件信誉技术 、文件信誉技术、行为关联分析技术、自动反馈机制、威胁信息汇总）的服务功能也将更加细化。现在，我们已经基本研发完成文件信誉技术，预计在明年推出的officescan10.0中将会内嵌这一创新技术。这一做法，将会优化及提升云安全技术的应用效果，将80%的病毒特征码放到云端的服务器中，这样一方面可以增大安全防护的广谱程度，另一方面在客户端将释放更多的系统资源。

TechTarget中国：与传统防病毒对比技术相比，云安全具有哪些优势？

徐学龙：云安全可以弥补传统防病毒对比技术的不足，提供强大的防护效果。这主要表现在：

第一，应对Web威胁，传统反病毒凸显技术困境。根据AV-Test.org的最新统计，全球恶意程序已超过1500万个，每4秒就产生一支新病毒，其速度大大超过安全厂商病毒代码的升级速度，如果不能在防护速度上有所突破，整个病毒防护将严重失衡。

第二，应对Web威胁，趋势科技云安全正走出一片安全防护新天地。因为任何一个恶意程序出现在网络中，其所在的信息源的诸多属性都会昭示出这个恶意程序与正常文件的不同，所以趋势科技云安全正是基于Internet平台，采用云计算数据处理模型针对海量信息的边际属性进行计算，将信息源的安全风险计算出来，这样在用户访问的高风险信息时，就可以自动进行提醒或阻止，实现零接触、零感染。

第三，趋势科技云安全技术正是将传统的病毒代码手工制作的过程转化为一种利用服务器将网络威胁计算出来的处理机制，所以网络威胁就不再受人员、时间、空间的限制，不仅实现了与病毒产生速度相匹配的防护，同时在防护效果上也更加简洁。

综上所述，云安全这种新的安全防护技术必将被广大用户更广泛地应用。

TechTarget中国：2009年云安全的发展前景将如何？这项技术是否会被广泛采用？

徐学龙：云安全技术会在未来更加细化，将应用到每一项安全服务产品之中。我相信，在2009年云安全的普及率会大大提升。截止目前，趋势科技客户中超过90%的用户已经在使用我们的云安全技术。据云安全的后台数字显示：在全球范围内，中国用户访问中国站点，在被发现是高风险访问而被阻止的统计中排名第一。这一方面证明国内恶意程序的分布规模惊人，另一方面也证明，云安全技术在中国客户群中获得极高的认可度，云安全技术的防护威力正在充分体现。

TechTarget中国：面对持续增长的Web威胁，您认为企业和IT安全专家应该更加关注安全技术，还是安全管理？

徐学龙：对于安全技术与安全管理，我不认为这是个应该分开而谈的问题。它们更像是一个人的双手，具有同样重要的位置，它们将相互作用，密不可分。

技术与管理是企业安全保障的两个方面，缺一不可。之所以很多人将安全技术与安全管理分开而谈，那是因为在多年前，病毒数量有限，仅依靠安全技术就可以保障企业的安全。例如，选择一个技术好的杀毒软件产品，基本涉及不到管理上的问题，就可以实现对企业的安全防护。而现在，随着网络应用的加深、企业网点增加，已经形成了庞大企业网络体系，这自然导致管理问题的出现。仅仅依靠某项技术、某一产品已经不能保障企业的网络安全。所以说，企业和IT安全专家对于安全技术、安全管理都应同等看重，不容忽视。

TechTarget中国：2009年的企业IT预算将不可避免地受到全球经济危机的影响，但是面临持续增长的Web威胁，您认为企业可以缩减IT安全预算吗？您有什么建议？

徐学龙：全球经济危机对企业的各方面都将有所影响，IT支出中的安全预算也不排除在外。但安全方面的预算高低，在一定程度上不仅取决于经济状况，而且也源于用户的安全防范意识。

尽管有一些安全意识不足的企业会认为：在经济不景气时，加强网络安全建设是不适当的做法，但是有安全意识的企业，十分了解安全风险会给企业带来多少损失。因此，这

样的企业不但不会在经济危机的时缩减安全投入，而且还会加强企业的网络安全建设。例如我们的很多客户，在部署网络版防毒产品后继续采购硬件安全网关产品，对网络安全进行加固。因为，在不稳定的经济大环境下，保证企业安全运营、业务稳定发展显得更加重要。所以，安全防护的预算不应该被列入压缩支出的范围。

（作者：Tina Guo　来源：TechTarget 中国）

KPMG：数据泄露将呈上升趋势

管理顾问 KPMG LLP 最新的报告显示，受到信用危机的影响，个人和金融数据的丢失在 2009 年将会急剧上升。

基于目前的形势，KPMG 说随着信用危机的加深，全球受到数据丢失影响的人数将在 2009 年增长到 1.9 亿，而在去年是 0.92 亿。报告说从八月到十一月受到数据丢失事件（4780000 万起）影响的人数比前八个月中所有事件的综合还要高，相比 2007 年同期增长了 38%（3450000 起）。

KPMG 从 2005 年开始跟踪数据丢失的公告报告，并在“数据丢失晴雨表”中作记录。它的合作伙伴 Malcolm Marshall 承认这些数据只是反映了真实的数据丢失问题的一小部分，在很多国家有大量的事件都没有报道。

Marshall 说他预计在 2009 年，随着金融紧缩以及犯罪转向泄露信息以获取收益额的个人，数据丢失比例将会增长。他说：“人们可能会担心他们的工作和经济，所以犯罪人员就会抓住经济下滑的机会。”

据 KPMG 称，自从 2005 年，在全球范围内，已经有 1300 次数据丢失事件的报告，而个人数据方面则有 3.5 亿人受到工具。在 2008 年，有 427 起数据丢失事件报告，全球有 83000000 人手到影响。虽然受影响的人数比 2007 年减少了，但是超过一半（47800000 人）的 2008 年的受害者是在这一年的最后三个月收到影响的。

虽然在线购物不太可能受到数据泄露的影响，因为所有的信用卡丢失都是被消费品信用贷款法案（Consumer Credit Act）所涵盖的，Marshall 说，公司自身受到影响的可能性非常大。

他说：“一旦他们被卷入事件中，他们的风险就会无限大，而且为了避免再次事件的影响他们可能会作出功能不全的决定。”

最大的风险存在于和外包公司和子承包人共享信息。虽然 Marshall 没有看到公司内部主要的贸易处理合同的任何迹象，但是他说一些企业已经选择自己处理自己的 IT 设备而不是把这一过程外包了。“曾经出现过在 eBay 上出售硬件的事件，所以有些公司选择雇佣强大的团队，并确保数据经过合适的处理。”

他说数据丢失现在已经是全球问题了，而且将会继续恶化，并且即使最安全、最全面的控制也不能提供对所有可能威胁的绝对的保护。

Marshall 提出了一些问题，所有的企业都可以这样问问自己：

- 你知不知道你的数据来自哪里？
- 数据存储在哪里，如何使用？
- 如果发生了数据丢失，你有没有清晰的可采用的计划？

（作者：Ron Condon　译者：Tina Guo　来源：TechTarget 中国）

未来的安全威胁：2009 年企业攻击

本文基于去年的威胁和攻击，对 2009 年的安全信息简单预测。但是，今年和不久的将来要面对的新威胁和过去所面对的看起来类似。

无线风险继续

有很多种方法通过无线漏洞攻击客户系统，就像通过 Karma 和 karmetasploit 所看到的。Karma 是一种分析无线客户端安全性的攻击的工具；karmetasploit 是作为无线访问点和对无线客户端所有探测请求作出回应的工具。

我认为很多企业都是五年前捕获的 Wi-Fi 威胁携带者的。wire-side 攻击的概念在很多管理圈中越来越有名，但是这花了很长时间。当无线出现一段时间的时候，很多无线安区那策略都是简单的不要使用天然不安全的 WEP 策略。糟糕的是，需要更加关注其他的脆弱的协议和其他无线攻击的多样性。例如，我们传统地在一个网络边界内查看风险。随着我们使用无线连同扩展网络，厂商使用了新的协议和认证方案，例如不同的 TKIP， LEAP and PEAP。在企业中采用协议之前，我们需要全面的研究厂商所使用的这些协议。

操作系统攻击归来

虽然操作系统攻击的有效性和名声没有恢复 2003-2005 的水平，但是恶意黑客很可能还将重新发现操作系统漏洞。过去几年已经有很多研究是针对浏览器攻击，例如跨站脚本（XSS）、跨站请求伪造（XSRF）和 clickjacking。但是如果这些技术和操作系统漏洞一起使用呢？

我认为我们开始看到越来越多的混合威胁，他们以 Web 服务器和浏览器中的弱点为目标，而同时也对操作系统造成伤害。如果攻击者可以攻击一台机器，他们就能利用操作系统再攻击内部系统，这种攻击可以允许黑客在很大程度上扩大他们策略的伤害程度。因为

这种混合，我们需要开始识别可能的安全盲点，例如桌面上安装的应用。我们还需要开发可是识别服务器和操作系统上的应用中漏洞的机制。

更加关注杀毒产品

Metasploit 3.2 的发布是分水岭。随着安全攻击平台的能力可以自动编写恶意负载，现在攻击新手也可能绕过企业的杀毒软件。使用一些简单的命令，黑客就可以激活恶意软件，绕过目前大部分（还可能是全部）的基于特征库的杀毒产品。

这种趋势很长时间之前就开始发展了。但是，我认为 2009 年将会出现使用这些技术攻击目标位置的攻击。采用 Metasploit 创建部分的蠕虫或者就可以提供有限的功能，因为杀毒厂商可以很快的发布新的特征码。但是如果以特别的目的针对企业——例如国防部、信用卡公司或者用于卫生信息的公司——就会很快受到损害。不需要很长的时间和持续的攻击，黑客就可以使用 Metasploit 进入，或者他们想要的东西。

企业也可以选择寻找包含应用探索法的安全产品，这类产品通过对不合适行为而不是特征码的识别恶意软件。安全产品还可以包括应用白名单技术。

用户 Web 冲浪的更多限制

当很多企业都关注主要的威胁携带者的时候，有件事儿比其他的更加突出：企业用户 Web 冲浪。到底为什么很多公司都允许他们的用户使用互联网呢？我的理解是很多公司需要他们的用户可以做研究，但坏死很多企业允许这类活动是因为他们想要把环境变成“工作的好地方”。在某些观点上，每个公司都需要平衡允许用户上网和攻击风险之间的利弊。

目前我帮助客户解决的几乎所有攻击都是内部用户浏览带有恶意软件的网站造成的。目前，这是攻击者绕过企业采用的闪光的 IDS/IPS/NAC/AV 技术的最简单的方法。

即使企业需要允许特定的一部分用户访问互联网，也要使用现有的强大的方法。例如，可以通过分段 VLAN 把这些系统和网络中的其他部分隔离。

培训预算缩减

培训预算在2009年将会缩减，这一点毫无疑问。我认为很多企业都在削减安全资源，这更多的是收入和预算全面缩减的条件反射。信息安全不是不会发展的。威胁总是在不断地进化，而企业的安全员工必须随之发展。通过削减他们的安全培新预算，有些企业可能会落后。尽管如此，我认为在今年下半年将会出现安全培训预算的上升，因为企业开始认识到将出现的威胁的严重性。由于我们职业的动态特征，总是需要培训，保持与最新攻击携带者的一致，更重要的是进行防御。

很少厂商说："Hack Proof"

最后，只是一个小请求。最近我看到越来越多的厂商在使用这个词。对于将在产品销售商使用这个词等厂商我有一些简单的建议：不要这么做。你只是在向恶意黑客挑战，让他们攻击你的产品，而有了足够的时间和精力，最终任何位置都会受到攻击。这也是不依靠任何产品或者方法的深度防御对企业这么的原因。最后，企业应该总是要提防任何产品的产品销售口号，他们斯和很好很正确，但是他们可能是。

（作者：　译者：　来源：TechTarget中国）

2009 认证和访问管理：裁员和内部威胁

认证和访问管理专家在 2009 年将会面临什么挑战？随着世界经济的混乱的状态、市场的自我修复和裁员，违法的内部活动较之前更加强大。

所有行业的公司都已经开始裁员了。可能开始的时候是削减冗员，但是不可避免的有些公司将会裁掉一些优秀的 IT 和信息安全专家。对失业的技术人员不太容易接受的违法活动可能只比挨饿好一点儿。就像滴水穿石一样，犯罪也会增加，而犯罪也会更复杂，例如数据窃取和社会工程。虽然很难想象，犯罪活动经常是以前的拥有这类合法操作的员工所造成的，因为他们对失业很伤心。

认证和访问管理专家的挑战将会是保护数据，防御从内到外完全了解系统的前员工。

防御策略：前摄的 IAM 程序

上锁使诚实的人们保持诚实，也就是说在认证和访问管理中，账户终止使诚实的人们保持诚实。认证管理和信息安全专家将需要比以前更要细察账户终止程序，因为保留未授权或者前员工的账户的活跃以及允许对敏感或者脆弱数据的访问都是灾难性的。确保公司的每个个体账户都有更新记录，这样如果出现终止，所有这类账户都可以被删除或者禁用。

现在是提前准备的时候。评估和提炼现有的程序。自从上次评估公司的所有账户生命周期程序到现在有多长时间了？对程序的完整性有信心吗，这包括所依赖的外部数据，例如 HR 反馈？承包人的数据管理充分吗？及时吗？有没有合适的职责分配方式？被遵守了吗？如果这些问题的答案是不清楚或者不知道，警告管理并开始对程序的改进的评估。

IAM 和预算缩减：使用架构和文件存储

2009 年的另一个挑战是资金。2008 年的预算期望肯定要被忽略，因为很多公司都需要根据新的经济现实作出调整。那么在资金不足的情况下，企业应该如何保护数据呢？改革。设立有效的架构，甚至是手动的加强。例如 Excel（或 Outlook）对系统所有者的季度报告详细说明了账户的访问权限、识别所有者和合作者、建立任务和安全的文件共享上的档案邮件。这将会触发将来会被优化的正在使用的程序，当经济状况转好的时候可能使用更先进的技术。

还有一些其他的重要策略，可以确保安全程序不会因为经济的削减受到损害。如果已经对员工每天的活动进行了详细的记录，现在就是这些信息盈利的时候了。它会不仅允许你证明为什么每个人都很重要，而且还要清楚的说明如果减员了，后果是什么。人员的减少可以委托办理的，但是数据可以帮助你不偏颇的做这些艰难的决定，并在开始就对减员的影响建立管理上的期望值。

要保留的重要统计可能包括有多少可以管理的帐户、帐户创建和移除的转变时间、各部门报告的要求，以及大型机资料和 Active Directory 组等管理对象。如果过去没有保留这些统计，从现在开始记录，探后选择可以帮助管理的数据，以最好的方式查看安全团队。基于事实的说明最难的工作不是傲慢自大，而更重要的是可以减少一些人的工作。

总结

在这样艰难的经济条件下，外部的威胁也会增加。将会有大量失业的优秀开发人员肯能发现他们的技能可以让他们成为优秀的程序员或者黑客。这些威胁太多了，在这里很难详细说明，确保减弱外部威胁的控件也已经评估过了，这样的警戒也很重要。

很显然，2009 年将和 2008 年产生极大的差异。依赖与过去经过验证的优秀之处，但是也要准备好基于新的威胁和业务需要裱画的快速改革与改良。

（作者：David Griffeth　译者：Tina Guo　来源：TechTarget 中国）

经济困难时如何保障安全预算？

问：华尔街危机好像要对整体经济产生长远影响，所以作为一名安全经理，我被要求缩减预算。你有没有什么办法帮助保护预算，特别是因为我们没有包含所有的基本情况？

答：预算被缩减很合理。在经济紧张时期，即使安全团队也要节约度日，并且多少要采取些措施。是的，即使不是每件事情都要这么做。所有接受这个事实，并向前进。

在经济低迷时期首先要考虑的要素是什么最重要。怎么才能知道什么最重要呢？询问高级管理团队吧。询问业务的优先等级、提出你的问题，确保他们了解了使用现有的资源什么可以做什么不可以。这就可以对哪些可以扔掉的东西提供了深入的了解。一旦清楚了哪些绝对需要保护，然后开始工作确保这些都已经执行了。

在开会前，应该建立三种不同的资产。第一种是哪些工作必须作。这个可能不会发生，但是表现全面的资产选择是为了更好的对比。第二种情况应该关注应该合适保护的资产的合理理由是什么？这种情况应该奋力争取，但是如果没有发生也不要失望。记住，时间很短。

最后，是最糟糕的情况。这是资产的绝对极小值，这是需要保护关键的资产。还有，需要清楚如果安全团队没有获得最小资产值的情况的细节。

附加的情况：当把上面三种情况都提交给管理层时，我建议要有第四种情况，也就是“紧急迫降”的情况。这是可能允许成功所需的最少的资金。如果安全团队连这种层面的资金也不给，然后就应该再找一份工作了，因为关键数据和系统受到攻击就只是时间问题了，而当这种情况发生时，还留在这里就不好了。

（作者：Mike Rothman 译者：Tina Guo 来源：TechTarget 中国）