经济危机下的 IT 安全

经济危机下的 IT 安全

2008 年的爆发的经济危机，影响遍布各行各业，IT 也受到很大的冲击。经济不景气总是犯罪的最佳时机，对敏感数据、客户和架构的威胁都在大幅增加，恶意网站、不满的员工、控制不好的合作伙伴、安全预算的缩减，各种威胁的频繁出现等都给安全带来了更多的不稳定性。那么企业面对这样的形势，应该怎么作呢？本专题综合了一些安全专家的意见和建议，希望能为企业的安全形势提供帮助。

危机下的安全形势

困难的经济时期一般和大幅裁员、合并和收购相关。越来越多的这种活动对数据安全造成了潜在的威胁，但是大部分的安全专家都认为大型公司都有适当地程序，确保主要动荡时期的安全和数据的完整性，但是内部威胁等越来越受到关注。

- 经济低迷 IT 安全专家关注内部威胁
- 2009 认证和访问管理：裁员和内部威胁

安全预算削减

不稳定的经济正促使很多公司削减预算，而对于还没有被要求减员或者降低预算的安全经理来说，现在应该开始起草可能削减预算的意外计划，并考虑如果出现 5%、10%甚至更高的预算缩减，他们应该如何处理。

- Forrester：经济尽管低迷 安全支出攀升
- 网络安全 2009 趋势：合并与安全预算缩减
- 经济虽然下滑 安全行业薪水上扬

安全预算缩减的应对

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，并且要采取些措施。安全经理首先要考虑的要素是什么最重要，本部分提供了如何合理利用安全预算，并提供了一些低成本识别网络攻击和控制无线访问的方法。

- 经济困难时如何保障安全预算？
- 预先识别网络攻击的低预算方法
- 控制无线局域网访问的紧张预算

经济危机时的安全策略

经济萧条、裁员以及对敏感数据、客户和架构的威胁都在大幅增加都促使企业以及安全专家调整安全策略，通过低成本技术和方法的使用维护企业安全状况。

- 经济危机时 四种方法区分安全项目的优先级
- 经济危机时 企业安全十技巧（一）
- 经济危机时 企业安全十技巧（二）
- 经济危机时 企业安全十技巧（三）
- 如何管理离职用户帐户

经济低迷 IT安全专家关注内部威胁

困难的经济时期一般和大幅裁员、合并和收购相关。越来越多的这种活动对数据安全造成了潜在的威胁，但是大部分的安全专家都认为大型公司都有适当地程序，确保主要动荡时期的安全和数据的完整性。数据安全厂商 Informatica Corp.的总裁兼首席安全官 Clardiu Popa 解释说合并和收购强制 IT 安全专家关注内部威胁。Popa 列举了一些确保不稳定时期的数据安全和用户信任的策略和最佳实践。

面临合并和收购（M&A）的公司在安全方面的最大挑战是什么？

Claudiu Popa：合并和收购是公司的敏感时期。这个时期信息资产的风险受几个因素的影响而增加，例如实施的不同策略、人员、无效程序、领导的中断以及不严格的安全控制。这种情况下的过渡时期最后导致的不仅是安全泄露，更严重的是使其更难检测。任何进行合并和出售的公司都必须测试他们的商业连贯性计划、他们的安全相应程序以及验证他们员工的安全意识等级，准备过渡时期。

最后，这个过渡时期关键的一个方面是不可避免的反复，以及对内部安全的影响。无论员工是因为不满，还是只是感觉没有人看到，加强安全监控和回顾员工协议绝对必要。但是因为项目众多以及变更管理的挑战，企业和行政人员把安全放到的规则基础上。部分原因是很难找到这种服务的出色的安全咨询人员。需要找到提供包括基于标准的安全项目管理（SPM）的公司。

对于那些不能继续业务可能被收购的金融公司而言可以采用那些数据安全措施？

Popa：我们在金融行业看到的这种类型的裁员和合并是一些严重的问题的起因，因为在有限的时间内这么多的人才和金融数据的易手导致每天都会发生错误。这些公司的客户需要询问他们的机构的属性和他们存储的可以确认的个人信息量。公司的客户也应该每月都审查银行的状态，尽快发现安全问题。不幸的事实是在企业变更基本方式的情况下，代

表巨大公司价值的信息资产可能首先被错放或者被窃取。很难判定这些信息是否用用于欺骗或者其他的非授权的目的。

我了解到金融公司比其他行业根甘泉，但是在经济危机时期公司的安全状态会降低吗？

Popa：整体上来说，当经济遇到公司的架构、所有权和操作都变化的时期，企业和信息安全的状况也不太好。不幸的是，最后的安全和隐私修楼趋向于影响公司的声誉和责任状态。如果有适当地标准控制架构，金融组织就可以防御、检测并控制潜在的灾难。

在合并和收购过程中，收购的公司多块可以并应该执行实践和策略？

Popa：收购的公司必须在并购前进行全面的教育、文件和指导方针的沟通和解释。两边的员工都需要知道策略、程序、表转和指南，确保合并的顺利进行。人力资源部必须了解可能导致安全失误的义务和责任。员工和管理人员必须明确地了解哪些信息他们可以带走，哪些必须过渡。第三方组织和咨询必须慎重管理、防御信息泄露和安全问题。

我觉得还需要执行代沟分析。收购公司应该查找什么？

Popa：代沟分许的执行是在作为整个项目的一部分的风险管理中，而且由参与过渡的每个部门分别进行。关键的部门是那些广泛使用信息的部门，例如 IT、人力资源、客户服务和市场。策略、认知、监控，特别是法规标准上的代沟都被标记了，而且代表了整个组织内的安全地过渡和程序、技术相关的信息的基础。一旦完成了安全平衡，新的企业就可以关注他们的程序，执行策略，并持续监控安全状态。

确保数据完整性和安全性的最佳方法是什么？

Popa：成熟的信息安全管理程序是持续并验证保护信息的唯一方法。每个企业都需要采取数据分类策略，而这些策略可以使人员、程序和技术有效地处理企业信息。为了恰当地保护数据，安全专家需要采用标准化的控制架构。这个架构应该涵盖所有的安全因素：机密性、完整性和可用性。阻止对敏感数据的访问还不够。数据需要具有预防性、可检

测、可矫正和补偿控制来确定是不是有什么事情发生，数据泄露应该可以在最短的时间内被分析、包含和修复。

可以采用的最好的做法是把人员、程序和技术分开：人员必须培训、动员并了解安全威胁，以便作出保护数据的正确决定。必须改进程序确保安全，而不降低生产力和可用性。必须慎重的采用技术，保证它可以有效地保证安全而不是妨碍。在帮助减少和控制风险和其他对操作系统和被邀请用户的负面影响的安全措施下有一条的线，可以绕过控制，完成工作。精确的安全很难达到，但是一旦企业到达了成熟的水平，安全措施就不只节约时间和资金了，还可以改进可信性和效率。

(作者：Robert Westervel 译者：Tina Guo 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）

Forrester：经济尽管低迷 安全支出攀升

剑桥大学Forrester Research Inc.首席分析师Khalid Kark称，不稳定的经济正促使很多公司紧缩预算，但是持续不断的数据泄露新闻使数据安全成为大部分公司会议室的主要话题。在这次采访中，Kark分享了最近安全调查的细节，并解释了为什么预算紧缩对安全项目没有产生主要影响。Kark将在周四在波士顿举行的Forrester安全论坛中公布细节。

在Forrester安全论坛中将会讨论什么，特别是您？

Khalid Kark：基于我们以前的经验，我们的大部分听众将是行政人员和高级安全专家，所以我们将要主要关注具体的安全技术和相关的策略方法。

而我将要设计三个部分。第一，信息安全的进步：我们从哪里来，我们在哪里，我们要去哪里。第二，我将要谈论我们从最近的安全调查中得到的数据点，这些调查信息包括各种组织的预算、项目、主要关注的问题等。这是我们第一次公布这些数据。演讲的第三部分将涉及将展望未来五年的机遇和未来成功安装的详细程序。

你提到了安全预算数据。目前的经济会影响到安全支出吗？

Kark：是和不是。我觉得有几个部分受到的负面影响比较大。我们发现有些部分虽然没有增长，但是也没有减少——公司保持了他们的安全预算。组织的审查更详细了；厂商的循环周期越来越长。有些行业，例如运输（航空、汽车制造等），削减了预算，但是这是例外不在规则之中。我们发现安全没有受到经济低迷的重大影响。

一个原因是媒体。由于最近发布的安全数据泄露，他们得出了这样的观点：如果我们不在安全上支出，我们就得上报纸的头版。CEO等人对安全对他们的意义了解的更多了。用户的需求、市场的推动状况等都使安全成为你的业务的一部分。用户了解如果他们共享

数据，数据会得到保护，所以公司都有了前摄心理：让我们把安全做成竞争优势。用户迫使公司考虑外部压力和媒体对安全泄漏事件的报道。所以，这三个因素促使高级管理确定他们在安全中的位置，以及为了减轻这些风险支出的费用。

我们今天面对的主要安全威胁是什么？

Kark：目前我们要处理的最复杂的是我们的环境的复杂性。管理环境变得越来越复杂。我们需要保护的不只是一个边界。我们需要保护不同组织中的数据。复杂性来源于两个角度：有很多工具，要确保他们可以一起工作。还有，在越来越全球化方面，要控制数据的去向更难了。所以，第三方安全变得非常重要，而且信心中心的观点也很挣扎。很多公司在保护知识产权的数据和员工数据方面受到了挑战。

我们在处理目前的威胁方面，做的更好了吗？

Kark：是的。我忍我我们在把基础做的更合适方面做的更好了。我觉得恶意认识总是提前一步，而且他们总是找到一个方法破坏我们的配置。但是我发现我们在把基础做得越来越好。

目前的安全状况很黯淡吗？

Kark：安全状况不想我们想象的，或者我们被迫相信的那么糟。我觉得我们现在处于很好的位置。很明显，安全将会出现复杂性、变更和附加的挑战，但是我们的位置非常好。CISOs 已经有能力在他们过去挣扎的领域取得进步。最近的数据表明我们正在改进，并且在收购企业。

公司会推迟对某些安全领域的配置吗？

Kark：当然。我认为过去我们所做的是在工具和技术上花费精力，而我们也在继续这么做。依据我们的位置的不同，它也会不同。有些公司（行业）甚至没有基本的安全工具和技术，所以他们可能仍将购买这些工具和技术，并减少更成熟得工具和服务。另一方面，有些成熟的公司延迟了采用帮助他们采集数据的工具和技术的时间。关注特定问题的

工具、技术和服务将会增加销量，而广阔的场景和宏大的方法将不受欢迎。所以公司寻找可以帮他们立即解决问题，以后又可以扩展到其他领域的厂商。提供一套而不是单个解决方案的产品存在增长潜力。

（作者：Cynthia Duga　译者：Tina Guo 来源：TechTarget 中国）

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)

经济虽然下滑 安全行业薪水上扬

虽然在经济混乱时期，雇佣经理可能是比较保守的做法，但是最近发布的技术薪资数据显示了惊人的趋势：一些信息安全专家的薪资增加了。

根据 Foote Partners LLC 发布的 IT 技术人员和人正人员薪资指标（IT Skills and Certifications Pay Index），在 2008 年的最后一个季度中，未认证的 IT 技术人员的全面薪水在一个季度中降低了 0.5%——这是自 2004 年以来的首次下降。

但是，对整体 IT 技术人员的支出——涵盖了几种安全技术和认证——在第四季度增长了，表明企业对可以帮助他们渡过危机的人员和技术的关注度增加了。

Foote Partners 的创始人兼 CEO David Foote 说“这不是因为 CIO 要削减成本而退回到‘刀耕火种’时期。这看起来像是（CIO）在混乱和紧缩时期计算出来的结果，这是为了很好的在技术技巧方面投资，这些技术技巧不仅可以通过萧条时期，还可以保证（他们的公司）在萧条过去后他们的核心更强大，更稳固。”

那么在赤字时期，CIO 认为安全方面比较有吸引力的是什么呢？Foote 说虽然管理人员不可能担心以后几个月的增长和增加的利润率，他们有更多的时间关注他们公司已经有的数据，并保持数据在经济问题结束时的完整性的重要性。

很多公司都要面对裁员的问题，公司应该关注被裁的不满员工带来的数据修楼问题。Foote 说 CIO 可能会让安全专家采用新的数据泄露防护（DLP）产品，或者监控 IAM 系统来防御被裁员工攻击敏感信息。

Foote 说：“维护的关键是你支出的多少，甚至在经济不景气时期支出的增长、增加和收益。关键是你如何分配仔 IT 产品、服务和劳动力方面的支出。”

看看这些数字，公司似乎认为安全确实是明智的投资。在前三个月中所有的 IT 安全认证人员的薪水增长了 0.8，比去年增长了 1.9%。薪水增加最大的认证是 GIAC Security Essentials Certification (GSEC)，在 2008 年第四季度增长了 46.7%；Certified Ethical Hacker (CEH)，增长了 40.0%。 认证信息安全经理（Certified Information Security Manager，CISM）在上个季度也增长了 7.1%。在薪水最高的 IT 认证中，42 个中有 18 个，也就是 42.9%是安全认证。

对于没有认证的安全技术，网络安全管理在第四季度无增无减，但是比前 6 个月增长了 6.7%，比去年增长了 14.3%。还有，网络安全管理和报告中提到的“不同的项目安全技术”是在前三个月中未认证的 IT 技术人员中薪水最高的。

Foote 说：“（这种上升的趋势）有很多驱动因素，但是总而言之这表明了从上次他们做这项工作的时候到现在，IT 管理走了多远。这是在消极的情况下看到的积极的一面。”

（作者： Carolyn Gibney 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。所以接受这个事实，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）

预先识别网络攻击的低预算方法

问：我们公司正在寻找一些可以全线识别网络入侵的方法，并且已经试验了一些。可能继续使用的一种是在 DMZ 中把蜜罐和 IDS 合并使用。有更好的低预算的测试网络入侵的方法吗？

答：我非常赞同在网络上使用入侵检测系统（IDS）或者入侵防御系统（IPS）的方法。这种方法可以帮助检测出危害到网络的恶意流量。这方面更详细的信息可以参考 techTarget 中国的另一篇介绍：《企业应该配置网络入侵防御系统吗？》。

在另一方面，蜜罐特别危险。需要认真考虑一下为什么想要在网络上采用确定会受到攻击的系统呢？蜜罐的使用是和故意漏洞相关的，这样就可以研究攻击者的行为和方法。最后的结果信息可以用于增加网络的安全性。但是如果蜜罐的配置出了问题，攻击者就可以访问网络，这时候怎么办呢？采用蜜罐就是对攻击者的一种信号，邀请他们对网络进行渗透测试。除非你的公司是专注与安全研究方面的，否则就不要采用蜜罐。

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

控制无线局域网访问的紧张预算

虽然，WPA 和 WPA2-企业版本提供了功能强大的无线局域网访问控制，但是配置 802.1X 对员工和预算有限制的企业而言具有压倒性的吸引力。从外包到开源，再到预共享密码，本文中，TechTarget 中国的特约专家描述了几个不太复杂或者费用较低的相关产品。

外包 802.1X 服务

WPA 和 WPA2-企业版本使用 802.1X 端口访问控制框架，验证无线用户。在企业网络中一般可以一起找到带有认证服务器的框架，比如 RADIUS 服务器、Windows 活动目录、RSA SecurID 认证管理员和认证授权。没有认证服务器，并且不愿意安装认证服务器的公司可以将这个组件外包到服务提供商，比如 McAfee 或者 Witopia。

这些供应商提供管理 Wi-Fi 认证服务。你的接入点可以通过 TLS 信道、跨因特网，将 802.1X/受保护 EAP 的信息转发到供应商的 RADIUS 服务器，而不是咨询你的本地 RADIUS 服务器。在准许或者拒绝访问你的无线局域网之前，这个服务器可以验证工作站的身份和密码。通过管理员网络入口，可以在你的帐户中添加或者移除用户名。

这些服务的细节有些差异——比如，McAfee 使用安装好的客户端软件或者客户向导来配置 802.1X 参数，而 Witopia 用入门指导自己进行安装。McAfee 用与 WPA-企业版相一致的参数来配置你的接入点，而 Witopia 是由你自己来为 WPA 或者 WPA2-企业版配置接入点。无论哪种方法，基本的设置都非常简单。外包 802.1X 服务，你就可以比配置“个人”预共享机密略多一些的精力便可以实现“企业”安全。

有了管理服务，就又出现了费用问题。Witopia SecureMyWiFi 开始一个接入点和五个用户，每年需要 29 美元。为了包括多于五个接入点和 20 个用户（每年 84 美元），需要进行报价。对于一个受保护的网络，小型企业的 McAfee 无线安全每月需要 4.95 美元；对

于五个或者五个以上的网络，每月降到了 3.99 美元。通常都会有试用版下载、促销和批量折扣，因此要查看供应商的网站，以了解现在的价格。

构建你自己的 802.1X 基础设施

一些公司宁可构建自己的认证服务器，但是缺少预算来购买商业版的 RADIUS 产品。另一种方法就是考虑使用免费的 RADIUS 服务器，比如 FreeRADIUS 或者 TinyPEAP。但是不要欺骗你自己：配置自己的 RADIUS 服务器需要更多的硬件、技术人员、以及至少需要一些辛勤工作。

为了运行 FreeRADIUS，你需要额外的运行 Linux、FreeBSD、OpenBSD、OSF/Unix 或者 Solaris 的时间和服务器硬件。FreeRADIUS 是在 GNU 通用公共许可证下发布的，这就意味着 FreeRADIUS 可以免费下载和安装。当作为无线认证服务器使用时，FreeRADIUS 可以处理 EAP-MD5、EAP-SIM、EAP-TLS、EAP-TTLS、EAP-PEAP 和 LEAP 的访问请求。你可以决定安全策略、服务器配置和用户证书。但是如果你一旦付出了努力，你就会拥有一个灵活的 RADIUS 服务器，可以用于其它用途，比如远程用户 VPN 认证。为无线网配置 FreeRADIUS 的相关建议可以在这里找到。

另外，TinyPEAP 是一个特殊用途的 RADIUS 执行工具，可以在 Linksys WRT54G/GS 无线路由器或者 Win32 系统上运行。当 TinyPEAP 安装在兼容的 Linksys 路由器上时，它可以格式化（over-write）厂商的固件，用一个带有非常小的内置服务器创建一个路由器。当 TinyPEAP 安装在 Windows 系统上时，可以创建一个小型的 RADIUS 后台程序，附近的无线路由器可以进行咨询。在这两种情况下，TinyPEAP 都只支持受保护 EAP 认证，对照用户名和密码的本地列表，检查 802.1X 请求。尽管 TinyPEAP 并不开源，但是测试版的二进制文件可以免费下载。

完全跳过 802.1X

一些受到 802.1X 的全部理念吸引的公司使用 WPA 或者 WPA2-个人版。当以功能强大的预共享密钥（PSK）为基础时，这些“个人版”的措施仍然代表 WEP 的一种改进。

当 PSK 太短或者由字典中可以找到的单词组成时，就可以很容易猜到。攻击者一般只需要捕获一些合法用户在连接到无线局域网时交换的信息包，然后运行一个字典式攻击工具，比如 CoWPAtty。为了预防这种攻击，选择一个至少由 20 个随机的字母数字字符组成的 PSK 值。为了获得最佳效果，使用一个随机密码发生器，并且确保包括数字和混合的密码（比如，T2adREfasACach64a6Us）。

不论你的 PSK 多么的随机或者有多长，每个连接到你无线局域网中的用户必须知道这个密码，或者将其配置到他们的系统中。设定好的密码可以使得生活更便捷，因为他们无需记住或者正确地输入一长串的随机字符。但是如果一些人丢失了笔记本或者密码无人看管时，这个设定好的密码就会受到威胁。另一方面，提示输入 PSK 增加了如下情况发生的机率：用户将密码告知客户、将密码写在便签上或者透漏整个无线局域网的密码。

虽然，定期更新你的无线局域网 PSK 可以减少风险，但是，组密码最终只能到此为止。如果你的公司真正在乎如何使外界无法进入你的无线局域网——或者及时了解什么人在哪个端点正在使用你的无线局域网——那么，升级到 WPA 或者 WPA2-企业版。

（作者：Lisa Phifer 译者：李娜娜来源：TechTarget 中国）

经济危机时 四种方法区分安全项目的优先级

经济萧条正造成全球的 IT 部门重新评估安全项目。这就必须作出一些重要的决定，即在维护健康安全状况的同时，在哪里削减安全投入。IT 和安全厂商可以使用四种方法区分安全项目的优先级，并重新评估销售前景的价值。在萧条时期，这些艰难的决定非常重要。

支持推动新收入来源的项目

对于大部分企业来说，业务顺序的第一条是使新用户的获得和保留变得更简单，这是安全方面需要投资的第一个地方。在保护使用 Web 应用的项目中 IT 继续排在前列，因为它可以抵消将来可能收入的所需的费用。身份和访问控件的安全产品、客户数据的保护以及 Web 流量的检查是扩展应用访问的本质因素。安全厂商将需要利用 Web 和云应用有效地扩展业务信息。

通过技术推动主要费用的节省

IT 企业要考虑的第二个问题是通过技术使用的革新推动实际成本的节约。这种类型的项目优先考虑成本节约和 IT 执行力。虚拟应用服务、远程访问和云服务等主要趋势可以节约企业的资金。允许 IT 降低管理成本的安全技术，例如配置控件、命令和控制服务器白名单以及虚拟机应用的审计也可以在这里发挥作用。

满足强制性法规要求

所有大型企业都必须遵守某些安全强制性要求。他们必须这么作，但是他们可能不喜欢。这些项目使他们使用最少的资金清除法规的障碍。在定义单项优势软件（best-of-breed）要求的时候，与产品功能和性能相比，IT 可能会增加管理费用和产品价格。导向审计控件和自动法规遵从报告的安全产品在这一类中都是很合适的。

替换表现不佳的产品

下一个有吸引力的安全投资种类是替换配置的产品。这类产品还没有老化，但是不能再有效的支持业务。当有其他很多种可以带来业务利润的机会的时候，IT 不喜欢技术上的再投资。这种类型的安全产品包括可以记录事件的 SIEM 产品或者需要改善性能的防火墙。对这些项目紧急性的认知，企业与企业之间又有很大的差别。

IT 可以把企业项目分为四类，然后查找每个项目中安全事故的防御、删除、审计和控制的安全技术。在这种训练的最后，安全团队将产生区分业务优先级的活动计划，同时也增进了安全的有效性。在这种经济形式下，安全厂商必须对他们的价值进行极其诚实的评估，并恰当地管理业务活动。“必须拥有”的产品的厂商列表在 2009 年会缩短很多。

（作者：Eric Ogren　译者：Tina Guo 来源：TechTarget 中国）

经济危机时 企业安全十技巧（一）

对善良的人来说目前是困难时期，但是经济不景气总是犯罪的时机。对敏感数据、客户和架构的威胁都在大幅增加，从威胁到恶意网站到不满的员工到控制不好的合作伙伴。

还好可以同时绷紧安全和经济。快速的决定策略可以帮助在不忽略网络架构的情况下走在进化的安全威胁之前。

有些灵活的方法可以使用。本文将介绍安全威胁管理状态的 10 个步骤，这些步骤只需最小的投入和人力就可以获得迅速的回报。

1. 保护切断能源的交换机

只需很少的精力，就可以锁定不使用的网络端口，而同时通过在不需要时关闭开关或者断电减少全面的能源消耗（例如从 Adtran 到 D-Link）节省资金。在新设备上的投资可以在一年或者更短的时间内获得收益。

自动关机是保护不使用端口的好办法，可以通过阻止窥探的电脑进入网络中的意外位置。这样还可以帮助实现物理安全，特别是在公众可以接近的建筑中，例如医院和政府办公室。

2. 寻找低成本的端点安全产品

很多端点安全应用或者代理的价格很高，而且交货时间较长。

如果想要取得好处而没有成本等困扰，那么一个解决方案是购买激活 TPM 的笔记本电脑，并使用某些形式的保护措施，例如存储在 TPM 上的指纹扫描器或者加密密钥，来拒绝非授权用户。这种合并是很有效的方法，因为 TPM 可以确保其他任何人都不能使用扫描的指纹访问笔记本电脑。

还有，考虑使用 Napera 或者 eEye Digitial Security 的 Blink 软件。他们都是低成本的端点安全产品趋势的代表，而这些产品都是 Windows 环境中的替换解决方案。

Napera 看起来像是网络交换机，并且可以和交换机上的代理软件与固件的结合体一起工作。可以在不同的端口上激活保护并确保连接到这些端口的每个电脑都更新了反病毒特征库和操作系统不定，而且在连接到网络之前没有恶意软件。24-port 设备的价格是 3500 美元，所以对很多小企业来说很有吸引了。或者它可以配置保护企业的公共区域，例如会议室和来宾室，这里有很多未知的笔记本连接到网络。

Blink 每年都可以为超过 30 位以上的保护，包括个人防火墙、杀毒和主机入侵防御模式等单点代理的一部分。

3. 获取免费 VPN

如果你还没有使用 VPN，现在正是开始的时候。随着移动员工的增多，暴露到 Wi-Fi 热点或者宾馆的可能性越大。当要在扩展网络在互联网上共享的时候，VPN 也可以发挥作用，并可以在路上访问文件。

当然，也可以在 VPN 技术上指出上万美元。但是如果只想要基本的简单保护，有很多低成本或者免费的软件的选择也可以成功实现，只要有可以支配的宽带连接。可以在 OpenVPN.org 获得开源工具。LogMeIn's Hamachi 是另外一个个人免费使用（否则每月需要支付很低的费用）的服务，并且安装建但。FileShareFreak 上还有一份清单可以提供其他工具。

技巧就是在公司内部普及使用这些 VPN 产品，并为首次使用 VPN 的用户提供支持资源。免费的 VPN 产品还可以作为价格更高的专业 VPN 的踏板，以及决定购买是否合适的方法。

4. 避免“思科税费”

在新年里，应该查看思科提供的年度支持费用，这些费用主要用于保持与 IOS 版本保持一致和维护响应时间上。我把这个叫做“思科税费”，你应该考虑是否应该购买替代设备备用或者寻找不会因固件/路由器操作系统软件升级而收费的其他供应商（Adtran 就可以考虑）。虽然在前期会产生一些费用，但是这样做能够快速收效。

5. 部署简易加密

当然，加密也是“容易做到，不易做好”技术之一，而且一直都在清单上出现。不过，近年来，出现了很多免费或者低价的邮件和磁盘加密工具，因此今年企业们应该开始真正实行对可移动磁盘和电子邮件的加密。

这里提供两个很好的选择：免费的开源软件 True Crypt 和 Voltage Security 的低成本但易于部署的 Voltage Security Networ 服务。

TrueCrypt 的磁盘加密客户端可以对 Mac、Linux 以及 Windows 系统进行加密，虽然该加密软件缺乏企业级管理工具，不过对于小型企业、管理人员和工作组而言，是不错的选择。Voltage 提供的电子邮件加密不需要安装任何客户端，可以与 Outlook 和 Webmail 结合使用，价格为每年每座 65 美元，Voltage 能够处理所有管理细节，并且托管服务能够轻松快速地执行。

另外就是 PGP 公司的加密产品，价格为每座 100 美元以下，取决于用户选择的功能。所有这些产品都是加密密钥管理变得非常简易 u：部署企业级加密的缺点就是，很难处理员工离开时的过期密钥或者员工忘记密钥时恢复密钥的问题。

同样可以分别为 windows 系统和 Mac 系统选择 Bitlocker 和 FileVault，这两种产品能够提供额外的保护，而不需要花费额外的费用。但是它们很难在整个企业进行部署，毕竟一分钱一分货。

6. 了解 IDS

你可能会认为简单部署入侵检查系统就足够了，不过现在应该仔细了解 IDS，并根据公司特定环境调整 IDS。这意味着需要调整 IDS 配置，了解其报告和登录行为，并做一些基步分析。

当然，这样做现在还不够，但是想要避免最新的安全威胁，就有必要用更多时间进行 IDS 分析以了解入侵检测情况。如果你使用 Snort 作为主要 IDS，请访问 Richard Bejtlich 的 podcast 以及 snort.org 的论坛以获取更多相关知识。

另一个方法就是对公司的一两个员工进行培训，让他们了解系统特征和加强系统安全的方法。虽然培训费用在经济危机时期是首要削减的开支，不过它可以快速投资回报，增加少量资金可以为系统提供额更多的安全防护。

7. 真正禁止前员工访问

这里谈到的是裁员浪潮里所有员工，而不只是 IT 部门里的。对公司而言，目前最大的威胁来自曾经处于公司内部职员而现在失业的那些员工。研究表明，前员工可能成为公司的安全噩梦。从未改变任何关键服务器的密码？是不是多台机器使用相同的主密码？那么，现在就是改变行为的时候。

还应该对最近解雇的员工带来的其他风险进行评估。公司访问控制策略是最新的么？已经禁用了所有安全密钥、密码和访问代码了吗？这些员工是否仍然能够使用远程网关呢？现在是时候检查访问日志并确保已解雇员工的访问目录项已经删除了。

8.坚决防御 SQL 注入攻击

不可思议的是这种“古老”的攻击方式现在还在产生影响，甚至破坏这么多的服务器。SQL 注入基本上是通过未受保护的页面进入数据库的后门，黑客可以在没有任何编程知识和技巧的情况下创造和执行 SQL 注入。为什么 SQL 这么麻烦呢？

一个原因是真正排除 SQL 注入攻击需要几个不同部门的合作，共同努力确保没有忽略安全漏洞。另一个原因是，漏洞网站很容易被找到，特别是密码很少的几个 Google 快速搜索工具可以在不需要黑客通过探测进入网络的情况下就可以发现漏洞。

所以我们今年要彻底解决这个问题，认真检查所有应用，确保网站再也不会出现在被攻击列表上。进行审计，聘请专业咨询公司或者进行如何修复数据库/web 服务器程序方面的培训，防御这种不幸的常见攻击的发生。访问 OWASP.org 获取更多关于正确设置数据库访问以及网站存在漏洞的原因和发现方法。

另外，你也可以下载 Acunetix 的免费的 Web Vulnerability Scanner 和 HP 评估工具的各种试用版，如 Weblnspect 等。

也可以试用 modsecurity.org 的开源 Web App Firewall 软件。

当然，如果这些下载的免费扫描器开始时没有发现任何问题，并不表示永远没有问题，不过至少可以开始了解如何使用这些工具并了解的漏洞存在的原因。需要定期进行扫描，确保黑客没有创建后门程序。

9. 防止数据泄漏

一起数据泄漏诉讼就可能毁掉整个公司。随着穿梭在互联网上的数据越来越多，就有必要查看可以防止数据泄漏或者至少积极防御数据泄漏的低成本工具。Code Green Networks 以及 eTelemetry Metron SE 就是监控产品的两个代表，它们配置简单，并且和同类产品相对价格也很低。此外，它们还可以进行大规模安装。

当然，这是之前没有想到的支出，但是如果尝试过这里推荐的其他成本更低的方法，那么这个就是中度投资的好位置。

10. 让自己人找到创新解决方案

你可能会想为什么自己没有想到这个简单的方案。建立一个奖励制度，鼓励延伸的思考方式和调整安全状态的方法，可以让自己的员工使用并从他们的建议中受益。这可以在不聘请咨询公司的同时，提高士气。在遇到理解系统主要问题的时候，自己人才是真正的专家。对员工参与的鼓励越多，他们就做的越好。

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

如何管理离职用户帐户

在经济不景气的时候，很多公司都被迫对他们的职工模式进行重新架构，以适应商品和服务要求的削减。这表示将有大量员工失业，通常是高层管理指定的日期。为了帮助信息安全和 IT 管理专家操作在规模缩小时产生的混乱的环境，本文中 TechTarget 中国的特约专家将介绍管理减少大量系统帐户的基本方法。

删除用户帐户的挑战

在信息安全和 IT 管理的很多方面，在进行减员方面的注意事项很少或者没有。这就向负责用户帐户管理的人提出了两大挑战。第一个是确定和离职员工相关的每个系统上的所有帐户。第二个是在短时间内禁用或者删除这些帐户，甚至需要在几个小时内完成。

成功解决这些问题需要一些高风险的方法。通常，首先考虑用户较多的高风险的目标系统，例如存储了机密客户数据或者带有资金活动能力的系统；低风险的系统，例如账户极少的内部电话簿应该最后考虑。

删除用户账户的过程

在开始前，确定要删除的帐户。如果公司有 SailPoint Technologies Inc.的 IdentityIQ 或者 Eurekify 的 Sage 等产品，就会很简单。这些认证管理工具可以帮助管理员管理在不同系统上地终端用户的地相关的帐户，并跟据公司政策管理。这些应用可以帮助产生每个系统上离职用户的目标帐户。有些甚至向系统管理员发送删除通知，并自动向供应/反供应产品提供反馈。有了这些工具，第一个挑战就解决了。

如果没有人证管理应用或程序，管理员应该开始向每个系统请求要删除的用户。这项工作要花很多时间，取决于系统的数量。为了加速这个过程，在自动对比某个系统上的帐户和新近离职的员工列表之前就准备好脚本。

一旦在所有的相关系统上地目标帐户已经确定了，下一步就是删除或者禁用这些账户。查看公司已有的系统，决定这些账户应该禁用还是删除。删除是最完美的，但是公司可能需要保留账户，这可能会有些合理的理由。这些理由包括访问邮件的业务需要和查账索引的连续性需要。这些已经建立的程序需要尽可能的维护连贯性。

如果公司已经一个自动的 provisioning 产品，例如 IBM Tivoli 的 Identity Manager 或者 Oracle Corp.的 Identity Manager，这些应用可以根据默认的策略禁用或者删除账户。这就和正常程序的进行一样简单，而 HR 反馈产生一系列的基于员工雇佣状况、工作流程和 deprovisioning 策略的事件。

如果公司没有自动 provisioning 产品，或者如果只有一个，但是不能和所有系统挂钩，就应该编写脚本。这些脚本应该加入到第一步时产生的目标账户列表上。还应该在比较低的区域进行测试，例如在开发或者 QA；中断产品环境比引规模缩小而引起的中断更不明智。

提前编写了脚本，并通过就是很大的优势，可以允许合适的开发和测试——在匆忙的情况下，程序的自然组件经常会被牺牲。

删除用户账户的最佳方式

不管公司的终止程序是怎样的，和 HR 保持密切的联系都是必要的。通产来说，信息安全和 IT 管理都不能决定在标准策略之外如何处理账户。如果时间是在标准程序之外，安全部分不应该负责决定哪些账户要删除，或者账户应该在什么时间删除或禁用。例如，基于 HR 反馈的自动产品在早上五点删除账户，那么安全部门有权利在中午以特别的方式开始这一过程吗？终止的策略应该好好制定并公布。严格遵守政策，没有例外，除非有合适来源的其他书面的指导。这个过程应该尽量客观公正。

在离职的情况中，最大的痛苦在于删除那些应该保留的账户。要为这些情况留后路，例如可以恢复账户的程序。还有，确保服务台指导谁是活跃的员工，谁不是。不要给不满的员工有呼叫进来的机会，也不能把他或者她的账户开放或重新安排。

如果你的公司是面临的经济危机可能导致在几个月后裁员的企业之一，记住。除了数量之外，程序应该和大家类似。如果没有处理大量员工离职的工具和过程，就应该开始编写脚本，发现账户并禁用或删除账户，然后确定 HR 已经全面了解了这一过程。

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