尽管他们匿名活动，但他们已经找到建立关系网的方法，从而创立这个特殊团体的供应链。 面对这样的犯罪分子，安全厂商需要进行更多协作，需要强有力的安全生态系统，建立共同的信息风险管理流程。然而，当前的信息安全技术仍处于各自为战的状态，只能对信息进行零星保护，彼此间的缝隙为网络犯罪留下了可乘之机。 科维洛的看法，在最近发生的“ 六省市断网事件 ”就是一个很好的印证。两个网游私服之间为了争夺玩家，运用黑客手段互相攻击。黑客在没法黑掉竞争对手网站的情况下，干脆从域名下手，对域名服务商DNS Pod的服务器进行了狂轰滥炸。结果影响到该服务器上 10万个网站的域名解析服务，这其中最出名、流量最大的是暴风影音。网民对暴风影音等10万个网站的正常访问请求随即演变为一场灾难。由于DNS Pod的DNS服务器已经瘫痪，而用户的请求集体转向中国电信的DNS解析服务器，从而导致电信服务器很快就瘫痪了。中国电信检测到异常的网间流量，从而启动应急机制，对六省市断网进行处理。在黑客眼中，只有他们自己的经验利益，没有法律，也不在乎无辜者的受害。“ 唯有的办法就是通过厂商协作，让信息基础架构更安全、牢不可破 ”，科维洛说，“ 必须制定一个共同的开发进程，紧紧围绕这一开发进程，构建更安全的信息基础架构。要确保未来的新技术架构是围绕这一开发进程而进行的，要确保该进程是基于信息风险管理，而不是强制执行一些技术组合。 ”科维洛先生呼吁业界围绕三大举措充分开展创造性协作，并举例阐述了RSA就此所做出的努力： 共同协作制定行业标准。如由RSA、惠普和IBM牵头制定的密钥管理基础架构(KMI)标准. 实现技术共享。免费提供领先RSA

BSAFE加密软件开发工具的RSA共享计划(RSA Share Project)正是实现共享的范例. 基础架构中的直接技术集成和嵌入控制。 例如，RSA最近宣布与思科移动解决方案集成，结合安全智能与地理定位技术，帮助加速安全威胁识别和响应。RSA enVision平台可以从思科移动服务引擎抽取数据，从而为客户提供固定用户和移动用户的物理位置数据，以及他们在工作场所内外使用计算和网络资源的方式。这一集成可以向IT专业人士提供可操作的事件信息，包括实时的用户物理位置、连接到有线/无线网络的主机和设备信息，从而帮助企业改善IT运营，强化安全策略，更快地响应安全威胁。 RSA与微软的SharePoint环境集成，识别SharePoint信息加中的机密信息和关键任务信息，采运用RSA的产品加上EMC对 Microsoft环境的专家知识，对关键信息、身份信息和基础架构加以保护，同时保持SharePoint平台的安全性和可用性。 RSA与关联公司VMware集成，在Vmware新发布的vSphere 4云操作系统内启动“ 以信息为中心的安全 ”功能，为虚拟数据中心加速部署以信息为中心的安全。由于数据中心虚拟化，物理的边界和界限不存在了。包括防火墙设备在内的传统安全产品，通常要求所有网络活动必须通过几个固定的物理位置以便进行监测，与此相对应的是，虚拟化应用可以在物理主机之间进行迁移，以获得更高的资源利用率和更长久的正常运行时间。安全的规则变了。只有像这样加强厂商协作，才能让信息基础架构更安全。 RSA与母公司EMC的存储平台全面集成，让信息得到更有效的保护。例如EMC存储平台与RSA身份认证集成，加强对数据操作的控制。EMC存储平台与RSA enVision集成，使得enVision可以搜集EMC存储平台的日志，

以便进行存储平台的信息安全事件管理。 企业要安全先行 当前，由于很多安全厂商的解决方案还缺乏协作，网络犯罪分子有很多可乘之机。尤其是企业在采用新技术的时候，更容易暴露在高风险之下。科维洛援引IDG研究和顶级信息安全官的建议，提醒企业在采用新技术时，一定要安全先行。“很多企业日益成长为‘超级扩展型’企业，它们比以往任何时候，以更丰富的方式相互交换信息，”科维洛说道，“新生的Web技术、云计算、虚拟化、社会网络、移动通信等技术方案的快速采用，正在迅速消融组织和信息资产的传统边界。当前，企业的安全战略必须要进行重大转变，以确保公司能够实现削减成本和完成收入的目标，同时不会造成新的、具有危险性的业务漏洞。”科维洛的观点与IDG研究报告的结果一致，IDG针对收入超过10亿美元公司的100位顶级安全高级管理人员进行调查研究，该报告的结果显示，越来越多的企业热衷于全新的信息通信技术，但他们在部署这些技术的同时，却没有对关键的流程和数据提供足够的保护。IDG 报告的主要结果包括： 70%以上的被调查者认为新的Web技术和通信技术给信息交换带来了提升，使公司越来越向超级扩展型企业发展。多数被调查企业在过去24个月增加了虚拟化、移动技术、社会网络技术的使用，超过三分之一的被调查企业增加了云计算应用。 多数被调查的公司并没有采取任何战略对应用新技术所带来的风险进行评估。有些公司在使用新技术之前，安全团队甚至没有得到任何的通知。 超过30%的被调查公司已经有一部分应用或业务流程运行在云环境中，还有16%的被调查公司计划在未来的12个月内开始迁移到云环境中。在这些公司中，有三分之二还没有实施

云计算环境下的安全策略。 10个受访者中有超过8个感觉到削减成本和创造收益的压力使它们大大增加了暴露在安全风险下的可能性，并在过去的18个月中经历过安全事件。被调查企业均表示，需要改变和提高企业的安全战略，以适应超级扩展型企业的现状。 与此同时，RSA业务创新安全理事会本周公布了它的第四份报告《构建大道：在前所未有的风险环境下打造“ 超级扩展型 ”企业》。这份研究报告从实际需求出发，强调了企业在面临预算和资源限制时，不让创新技术面临安全风险的重要性。这份报告显示，顶级公司的领导者在促进创新的同时，还不忽略企业的安全实践和政策。报告总结了世界顶级安全官们的指导意见，提供了创建企业全新安全模型的七个步骤。内容包括： 在保护环境中进行限制。更加有效地利用资源的方式。限制安全资源对不相干的信息资产、存储数据、以及设备进行保护的战略。通过在保护环境中进行信息资源的限制，企业同时还能够降低成本，减少风险并释放资源，以用于高优先级的项目。 取得竞争力。在经济艰难的时候，如果企业领导人感觉不能从内部安全组织中得到他们所需要的，那么转向外部服务供应商，而不将公司安全团队包含进来将会增加企业的总体风险。安全团队专注于企业服务的质量和效率，并清晰了解购买服务的价格。 积极利用相关领域的科技。信息安全部门必须认识到阻止新兴web和通信技术的使用是不可行的.相反他们必须推动这些技术的安全使用。企业应该从被动安全措施转变到预防性安全措施。 从保护载体转向保护数据。在超级扩展型企业的时代，越来越多的企业数据都是在不为企业所控制的载体中进行存储和处理的。例如，数据可能在服务供应商的设备中

进行处理，或保留在员工使用的PDA中基。在这样的环境中，企业应该将信息安全的保护重点从设备转移到保护数据上来。 采用先进的安全监控技术。在今天的威胁环境中，安全团队必须对用来监测异常和恶意活动的方法进行升级。比如从基于签名的防病毒和黑名单方法转向基于行为的监测和白名单等更精确的技术。 协同创建行业标准。就安全技术人员、第三方供应商、以及新兴的技术建立统一的信息安全标准，已经到了一个关键的时候。 分享风险情报。为了使企业能够抵御国际黑客和日益复杂的欺诈网络，应该建立起一个涵盖企业，执法机关和政府的、强有力并具协作性的情报共享生态系统。 站出来的为什么是RSA 科维洛呼吁厂商进行协作，并得到业界的积极响应，得益于RSA的行业声望和品牌号召力。以目前的RSA 反网络欺诈指挥中心(AFCC)为例。AFCC已将网络钓鱼攻击的平均寿命从115小时减少为5小时。依据攻击的复杂程度而定，在许多案例中，在被 AFCC关闭之前，钓鱼攻击只活跃了几分钟。之所以有这么快速的反映，是因为RSA 反网络欺诈指挥中心(AFCC)与全球9000多家互联网服务供应商、多家计算机紧急响应组(CERT)和执法机构建立了直接与开放的沟通渠道。到目前为止，通过与全球超过4,500家网站合作，RSA 反网络欺诈指挥中心(AFCC)已在全球超过135个国家关闭了50,000多个Phishing(网络钓鱼)攻击。 著名分析机构Gartner最新公布题为《具有广泛产品组合的企业级认证解决方案供应商MarketScope》的报告，RSA认证解决方案唯一获得“ 绝对优势(Strong Positive) ”这一最高评级。 RSA认证解决方案深受全球用户的认可。全世界3万多家组织的4000万人正在使用RSA SecurID?双因素认证系统。仅仅在

中国，RSA就已经保护着1000多万个人和企业用户的身份，广泛覆盖银行、电信、电力、制造等多个领域。例如，总部设在台湾的集成电路设计公司立科技最近选择了RSA SecurID？双因素认证解决方案，以保护它通过研发获得的宝贵知识产权和客户的信息，访问公司敏感信息的员工需要通过RSA SecurID进行身份认证，而不仅仅是用户名和静态密码这样简单。 在2009年5月Gartner最新公布的《安全信息与事件管理(SIEM)2009魔力矩阵》中，RSA再次位列领导者象限。Gartner 对RSA的执行能力和愿景的完整性给予了高度评价。同样，在2009年2月Gartner最新发布的题为《网络欺诈检测魔力象限》报告中，RSA也位列领导者象限。根据Gartner的解释，这一定位基于RSA相关技术发展完整愿景和技术执行能力，该技术与RSA的身份验证和保护套件相关。 