浅谈新技术浪潮带来的新安全隐患思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/607/2021_2022__E6_B5_85_E8_B0_88_E6_96_B0_E6_c101_607201.htm 近日，RSA公布了两项新的研究报告，报告对很多现在新兴技术所显现出来的深远安全问题进行了研究分析。第一项研究报告是由IDG公司研究服务部门进行的，该报告揭露了企业采用全新的连接、协作和通信技术的匆忙速度，与安全部署这些技术的准备状态存在着巨大差距。第二项是有关RSA业务创新安全委员会的研究报告，它概述了企业如何利用这些新兴技术带来的商业优势，同时不会使公司陷入风险之中。 RSA总裁Art Coviello说道，“ 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，新生的Web技术、社交平台和移动技术的快速采用，以及越来越普遍的外包现象，正在迅速消融企业和信息资产的传统边界。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达到收入目标的目的，同时不会造成新的、具有危险性的业务漏洞。 ”IDG公司研究服务部门进行了一项调查，调查对象主要是收入超过10亿美元公司的100位顶级安全高级管理人员，结果表明有些企业太热衷于新兴Web和移动技术，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。 主要调查结果包括： 70%以上的被调查者认为新的Web技术和通信技术给连接和信息交换层带来了提升，使他们的企业越来越向超级扩展型企业发展。在过去的12-24个月中，多数被调查者都增加了虚拟化、移动、社会网络技术的使用，超过三分之一的被调查者增加了云计算的

使用。 但是，许多接受调查的公司并没有采取任何战略对采用这些新技术所带来的风险进行评估。在一些企业中，企业的安全团队只有在发生问题时才会被要求介入，而在其它时候，使用这些新技术之前安全团队甚至没有得到任何的通知。不到一半的被调查公司已经制定了相关的政策，以指导员工如何使用社会网络工具和网站。 30%以上的被调查公司已经有一些企业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。 80%的受访者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。70%的受访者在过去的18个月中经历过安全事件。 大部分受调查者都表示，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。 研究结果在IDG公司研究服务部门的白皮书“ 随着超级扩展性企业的不断成长，风险也在日益扩大 ”中有详细的描述。企业们也可以对它们成为超级扩展型企业的安全准备状态进行测试，并将测试结果与受调查高级管理人员的结果进行对比。 顶级“ 信息安全官 ”表示，超级扩展型企业需要新的安全措施 同样在今天，RSA还公布了其业务创新安全理事会的第四份报告：“ 构建大道：在前所未有的风险环境下打造“ 超级扩展型 ”企业。 ”在这份报告中，来自世界各地的顶级安全领导者共同探讨了在今天这样一个原本能够推动新的商业价值的善意行动却会使企业置于灾难性风险之中的世界里，如何转变安全战略。 “ 在这个特定的时间点，如果我们有这样一个迅速变化的环境，我们绝对要哭，‘ 时间到! ’我们需要逐步走出来，我们需要检验计划是否进行了正确的

调整，”Diageo(帝亚吉欧)首席信息安全官、理事会成员Claudia Natanson博士表示，“您的计划是否为即将开始的艰辛困境作好了准备?因为只有最敏捷的，最胜任的，最灵活的计划才能到达终点。”RSA的前一项研究：“推动更快地发展：在严峻的经济环境下管理信息安全以寻求战略优势”，强调了在面临预算和资源限制时不要使创新倒退的重要性。这项新的报告演示了顶级公司的领导者是如何在促进创新的同时，还不忽略企业的安全实践和政策。报告提供了创建企业全新安全模型的七个步骤 在与业务创新安全理事会，世界顶级安全官的深入对话基础上，本报告着眼于信息安全的发展方向。它为开发一个能够反映即将出现的新机会和危险的最新信息安全模型提供了具体的建议。理事会成员概述了为什么现今的威胁环境变化莫测，并就如何安全地利用超级扩展型企业以创造业务优势共享了他们的建议。具体指导包括：在保护环境中进行限制。确定能更加有效地利用资源的方式。例如，理事会概述了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企业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。理事会解释了安全团队如何专注于他们服务质量和效率，并能清晰地阐明购买服务的价格为他们所带来的价值。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。理事会成员就

如何从被动安全措施转变到预防性安全措施，以及如何建立企业采用新技术的路线图分享了指导意见。 从保护容器转向保护数据。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容器中进行存储和处理。例如，数据可能由服务供应商的设施进行处理，或保留在员工使用的PDA，或拥有多个企业客户的承包商使用的笔记本电脑中。在这样的环境中，理事会对将重点从保护设备转移到保护数据上提供了指导。 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。理事会成员分享了从基于签名的防病毒和黑名单方法转向诸如基于行为的监测和白名单等更精确技术的建议。 协同创建行业标准。理事会成员就安全技术人员，第三方供应商和新兴技术建立统一的信息安全标准，为什么已经到了一个关键结合点进行了探讨。 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，理事会推荐了一个涵盖企业，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。 