风控官 及 信息安全官：一场对抗安全威胁的双雄战

Jacqueline Lee 2016 年 4 月 19 日

蝙蝠侠和罗宾，汉索罗和丘巴卡，夏洛克和华生。不管是在科幻小说，还是在真实世界，伟大的成就需要同样伟大的伙伴关系。纵观当今企业界，你会发现城市中涌现了一支全新的超级英雄团队：风控官（CRO）和信息安全官（CISO）。

CRO 和 CISO 对企业最高管理层而言相对陌生，他们将竭力帮助企业规避法律合规性问题和安全威胁。两者之间日益重要的合作伙伴关系表明，规避企业财务损失意味着要加大在信息安全领域的投资力度。

CRO 与 CISO 共同的目标

保险行业最先设立 CRO 这一职位，银行业和金融服务业纷纷紧随其后，也随即设立了 CRO 一职 。尽管金融专业知识对于风险管理仍至关重要，但如今的 CRO 必须从更宏观的层面来评估风险。

CRO 和 CISO 在安全问题和风险管理等方面面临着许多相同的问题。灾备报告称企业最高管理层最担忧的七大风险中，以下三个与信息安全有直接关联：

1. **法规变更和审查：**企业须遵循一系列法规，从《医疗保险可携性和责任法案》到《萨班斯-奥克斯利法案》，比比皆是。违背相关法案将增加数据泄露的风险，使企业面临债务和收益波动的多重风险。
2. **网络威胁：**网络边界安全、鱼叉式网络钓鱼、进阶攻击载体以及内部破解均会对企业带来巨大风险。入侵者想获得有价值的知识产权、员工和客户的敏感信息，以及公司当下的内幕消息。
3. **身份管理和隐私：**现代社会，员工通常可以在任何地点办公，因此远程网络访问必不可少。许多员工也会将敏感信息存储在个人设备上。这种灵活性能使员工更容易地完成任务，但同时也加大了重要数据保护的难度。

CRO 与 CISO 之间的密切关系能帮助企业规避一些成本较高的威胁。在安全术语的使用方面， CISO 与 CRO 有所不同，这使得 CRO 能更好地传达特定的安全问题。另一方面，CRO 能帮助 CISO 将安全威胁问题与潜在运营、战略和财务结果联系起来，从而加大安全支出的投入。

与高层之间的直接沟通渠道

普华永道会计师事务所称， 目前 90% 的公司采用基于风险的方法应对安全问题。提高安全

性、降低组织内部风险的关键在于让 CRO 和 CISO 直接与决策者沟通。

在许多企业 ,CISO 向首席信息官 (CIO) 汇报。通常来说 ,CRO 向首席执行官 (CEO) 汇报，也可能向公司董事会或首席财务官汇报。《华尔街日报》称，就 CRO 的职责而言，金融服务业是无疑是最具前瞻性的行业了，金融服务业中，68% 的 CRO 直接向 CEO 汇报，46% 直接向董事会汇报。

不管一个企业的组织结构如何严密，为 CRO 和 CISO 提供一条与高级决策人进行直接沟通的渠道至关重要。如果在 CRO 和 CISO 与公司高级管理人员之间的沟通有多重障碍，那么双方直接沟通的成本就会相当高昂。据 CSO Online 称，如果 CISO 向 CIO 汇报，而不是向 CEO 汇报， 企业宕机的几率将会增加 14%，与安全问题相关的财务损失几率也会增加 46%。

通常来说，与 CISO 相比，CRO 与企业最高管理层接触的机会相对较多，主要是因为企业最高管理层习惯用金融术语将风险管理概念化。然而 ,随着安全事故风险不断加剧 ,宕机、违规、商誉受损、风险管理的范围将超出金融知识，拓展到信息安全领域。财务损失引发安全威胁问题，CISO 成了灾后恢复功能和合规最有价值的盟友。

早在发生灾害之前，CRO 与 CISO 之间就形成了一种牢固互信的合作伙伴关系，这种关系将形成一个灾备盾牌，帮助企业防范毁灭性的财务损失。

作者介绍：

Jacqueline Lee

自由撰稿人

Jacqueline Lee 专门从事商业技术写作，在商业、管理和创业领域拥有长达 10 多年的经验。如今，她为 HireVue 和 IBM 撰写博文，她代表客户品牌撰写的文章曾刊登在《赫芬顿邮报》、《福布斯》、《企业家》和《企业杂志》等报刊上。除了写作，Jackie 还担任社交媒体经理和自由编辑。她还是美国编辑协会会员，荣获波因特研究所颁发的编辑证书。