网络风险之人的因素

与退休四星上将詹姆斯·琼斯（James Jones）相处一段时间，你很可能会听到他对“那些一直是和即将成为网络攻击目标的公司”发表警示观点。作为前美国国家安全顾问和海军陆战队司令，琼斯将军在职业生涯中投身于了解、减轻和预防各种安全风险。

几十年来，商业行业一直在积极对抗网络风险，然而网络攻击却变得更加频繁、严重。大多数人将网络犯罪与外部威胁、民族国家以及入侵公司网络的黑客联系在一起。公司针对抵御外部侵害、防止不法分子侵入投入了大量资金。但其实网络犯罪是公司内外因素共同作用下的结果。内部人士，即公司招募或雇用的员工，往往需要为经济损失和犯罪活动承担一半的责任。

根据犯罪理论，犯罪是动机和机会的结果。由于对内部威胁的担忧日益增加，多数机构几乎都将关注因素放在这一等式的机会因素上，即监控工作场所的数字活动、设置权限以减少犯罪机会。这种形式的内部网络监控对象可能包括文档、文件夹、文件和网站的访问与使用情况，以及内部电子邮件通信。这些措施的目的是识别、理解和记录可疑或非法活动，并限制或切断对敏感、机密或财务数据的访问。

把这看作是防守的最后一道防线。威胁已经出现。此时此刻，犯罪分子们正在蠢蠢欲动。目前的计划是以足够快的速度在活动初期便完成识别工作，以排除或避免犯罪机会，保护机构不受进行中的犯罪活动的侵害。

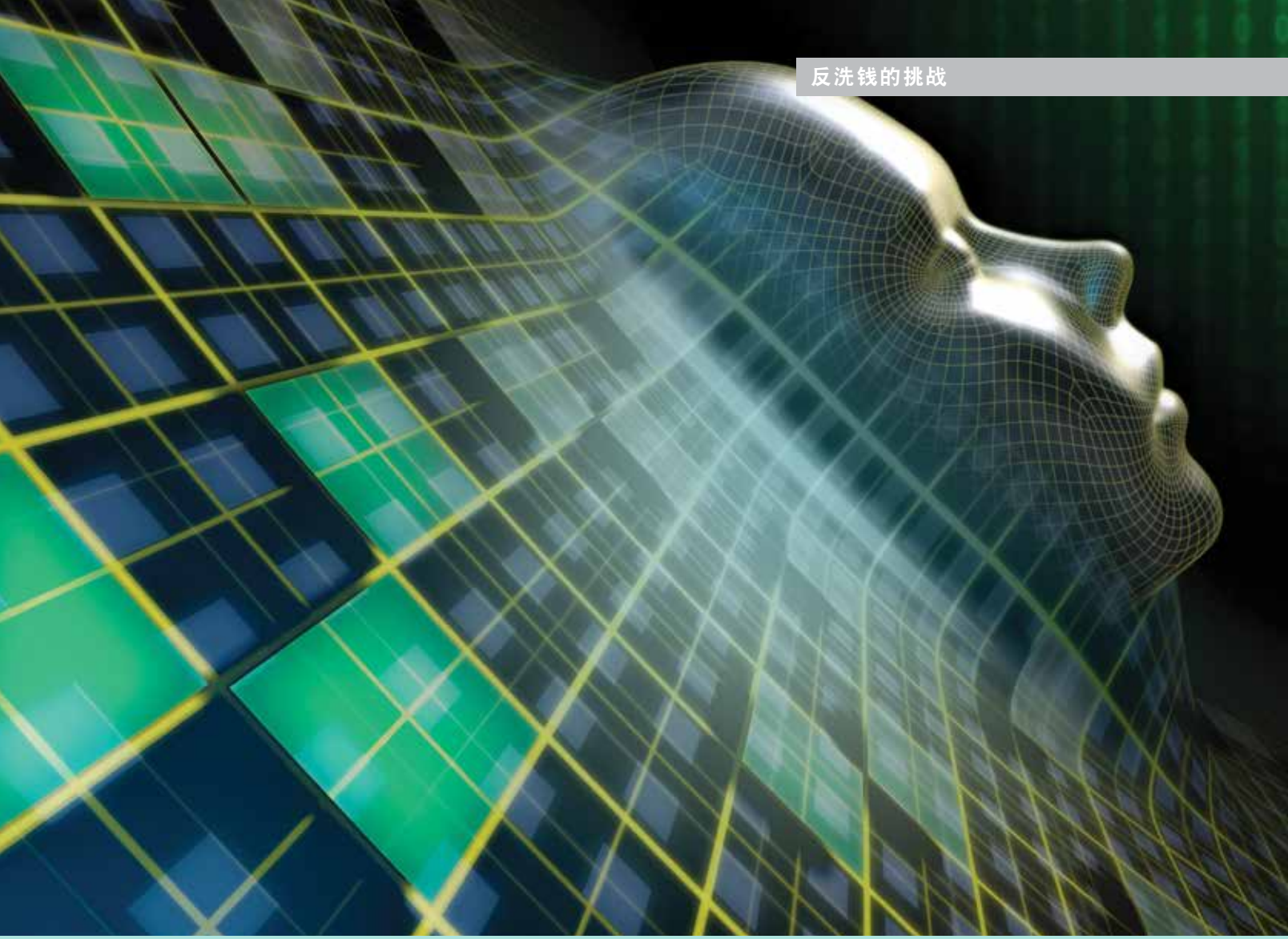
如今，公司不仅在抵御网络犯罪，而且希望通过将关注重点扩大到造成风险的人为因素上来避免内部威胁。大多数网络专家认为，人（员工）往往是一家公司网络防御中最脆弱的一环。许多机构认为员工风险源自击键时的疏忽或糟糕的网络使用习惯（“不要点击该链接”、“不要打开该文档”、“不使用‘密码’一词作为您的密码”）。这种人为因素造成的风险是缺乏教育或疏忽大意的结果。过失行为造成的风险可以通过适当培训和程序加以解决。

令人遗憾的是，并非所有人为风险都是由失误引起的。内部人士也会有意识地从事非法活动，所以公司必须对犯罪动机加以了解并进行解决。请注意，员工对公司实施欺诈或网络犯罪行为并非一时兴起。在工作场所的犯罪行为发生前，往往会出现一些特定情况或发生一些特定事件。

关键在于，公司需要识别出哪些员工容易实施违法行为，或容易受外部不法分子影响，成为获取经济利益的工具。这些员工都承担了一些犯罪、经济或其他个人压力，而公司对此并不知情。他们是公司内部最难以防范的威胁。因为作为内部人员，他们能够了解公司的防御系统并加以学习，从而避开或攻破这些系统的防御。

为了员工、同事和整个机构，公司必须始终了解员工在公司内外出现的重大行为转变。“了解您的员工”倡议强调，公司需要长期了解员工的整体情况，并及时辨别不寻常的高风险行为（例如在公司外部一再进行或升级犯罪活动、个人财务状况突然出现巨大变化等）。这类在招聘过程中就应认定为不合格的行为，可能会在六个月、一年或五年后出现，并一直不被发现，因此机构并未对此进行处理。

人们的生活总会因为一些常见的原因发生变化，比如结婚、生子、买房、搬家、照顾家人、支付学费或生病住院等。重大变化会给人带来一定程度的压力，而这种个人压力往往是暂时的，可以通过积极、建设性的行为加以排解。但是，有时过高的压力值可能会导致情况失控，而且在很多时候，家人、朋友、同事和主管们并不会注意到这种情况。



在网络风险管理问题上，对于人为因素的管理在本质上是以人为本的。任何机构都应该在保护机构的风险管理目标和构建信任文化的人事目标上实现平衡。尽可能多地积累员工数据（即通过辨别行为好坏以识别风险）并不是解决方法。此外，也不能通过每日重复背景调查或在员工离开公司时每日监控其日常行为等方式解决上述问题。

解决方案必须以事件本身为基础，可进行实时监测，具可执行性的，且其驱动因素应为可能对您的行业、公司和每一位员工的工作构成较高风险的具体行为。比如，财务总监因支票诈骗被捕、使用公司车辆的员工酒驾被捕，公司几乎一定认为这些行为是高危行为。某些角色确实很关键，需要及时发出警报以减轻风险。视具体情况制定策略很重要，因为不是每个员工都会接触相同级别的财务交易、客户个人可识别信息、信用卡帐户或敏感数据。

解决方案还须保障员工的权利和隐私。技术可以使执行过程规范化，确保遵守法律和法规，促进积极透明的网络风险政策，最重要的是应避免个人偏见和临时决策。这样就能在保护机构和个人上实现平衡。

最后，内部风险管理的目标并不局限于保护组织免遭网络犯罪。现在公司可以通过风险行为的领先指标及警示信号，协助那些没有发出帮助请求但需要帮助的员工。公司可以干预，通过培训、咨询或一对一交流积极引导，纠正员工行为。这样可以更好地确保员工在当前角色和长期的职业发展道路上获得成功。公司如果在内部风险真正威胁到员工工作或对机构造成实际威胁之前就防止它发生，就能实现最终的胜利。

Tom Miller，ClearForce 首席执行官，美国弗吉尼亚州维也纳，
tmiller@clearforce.com