Deloitte.
德勤

中国企业领导制高点
如何抵御网络威胁

虽然大部分的网络袭击事件均未至于成为国家头条新闻，但却足以对企业造成各式各样的伤害，轻则公司网站遭受破坏，重则导致网络中断、恶意欺诈、以及盗用知识版权。很多企业均需要建立规划方案，以整体预防及应对此等袭击行为，因此需要公司董事会及各首席级高管多加注意。

美国证监会（SEC）最近亦对此问题表示关注，董事会和首席财务官均必须参与有关过程，明白相关政策如何在企业各项战略的大前提下运作。美国证监会公司融资监管部最近发出公布，当中提及旨在“协助注册公司评估须就网络安全作出之相关披露（如有的话）”的指引。上述公布以〈公司融资披露指引：（二）网络安全〉[1] 为题，并补充“如同其他运营与财务风险，注册公司应不时检讨，确保已就网络安全风险与网络事故作出足够披露。”

虽然中国监管当局还没有推出类似的指引，但不少首席财务官与董事会已积极地寻找提升企业网络安全的方法。本期《企业领导制高点》将探讨如何加以利用风险智能分析网络威胁，并概述企业应采取的步骤，使网络威胁风险管治更为有效。

利用风险智能分析网络威胁

风险管理委员会和企业本身在应对财务、声誉与规管等各种不同风险时，均会提出上述相同问题。可是每当涉及网络风险，“网络威胁”一词往往被人误解，或是低估有关网络威胁的影响，因此以上高水平问题未能妥善解决，以应付相关威胁。

除非公司在网络威胁风险管理方面的实务已经达到相当精密的水平，否则未必具备风险管理架构及/或管治元素，以支持有意义的交流。例如就风险定义、风险承受能力或网络威胁风险的指定计量，公司领导层可能会有不同的意见。或是公司缺乏技术工具，以有效搜集并报告网络威胁相关资讯。对大部分企业而言，信息科技（IT）部门以外的高管人员与董事会成员的积极参与，亦可能具有一定的关键性。

假如企业尚未准备就绪，就有关风险与效益等事宜进行讨论，首要步骤是向高管团队就有效管理网络威胁风险必须的特定信息安全实务，提出以下四个问题：

- 如何追踪从公司发出的数码资讯，以及有关资讯的去向？
- 如何找出实际登入公司网站人士的身份，以及登入地点？
- 如何监控在公司设备内运作的软件？
- 如何限制我方在自愿的情况下，容许网络狙击手取得的资讯？

高效的网络风险管理流程可重复再用、具备明确清晰的规定与妥善文档，并配合企业更大型的信息科技风险管理（ITRM）与企业风险管理（ERM）框架。企业可计量并监察相关流程的效能和效率，并利用持续改善技术以提升绩效。

很多企业的网络安全实务均尤其着重各种措施，如防火墙和密码保护，旨在限制进入公司网络。虽然此等预防措施乃必须措施，但却无法提供足够保护。网络犯罪分子的技术亦越趋纯熟，能够避免触动相关警报，顺利入侵公司网络。除非公司刻意追寻可疑活动的蛛丝马迹，否则一旦成功进入网络，犯罪分子便可以在不经不觉间，轻易从网络上拿取资讯。

为打击那些避过监控入侵网络的犯罪分子，网络威胁风险管理程式或电脑传讯规则，应包括防止未经授权发布及取得资讯的内容。为求有效发挥网络威胁风险管理程式的功能，应实施相关 技术、科技与流程，以监察对外流传资讯的内容（是否适合对外分享？）及去向（被发送至何处？）。尤其是，关注资讯流传去向亦有警示作用；若有关资讯被发送至公司业务地点以外的国家，便应该查看发送人的身份以及其发送目的。高效的防御程式能够阻截可疑通讯，直至相关通讯成功通过核证为止。比如说，进行适当查证的同时，利用科技电子“封锁”相关通讯。

完善网络威胁风险管理能力的特征

风险管治 **（董事会）：**	**通讯：**与管理层保持沟通；双方就重要制度与关键业绩指标达成协议，并进行实时监控。
风险架构 **（归属高级管理层，负责实施与维持人员、流程与科技等需要进行风险管理“工作”的范畴）：**	**人员：** 高管团队具备相关背景知识与最新资讯，并在广泛的企业风险管理决策中，积极融入网络威胁风险之考虑；企业利用网络威胁智能，在已制定的风险承受水平内，协助管理各种类别的风险（不单是网络威胁风险）。 **流程：**持续致力改善流程，包括自动系统以及其他适当的促成技术；妥善建构的网络威胁风险管理程式，并融入更广泛的信息科技风险管理和企业风险管理程式。 **科技：** 自动化技术不但用于监察相关威胁与警示，而且更用于其他保安流程，如恶意软件、法证分析与威胁评估。
风险归属 （各个部门及业务单位）：	除了上述特征外，制定特别奖励制度；按照其网络威胁风险管理的表现，奖励相关主要人员。

提升网络威胁风险管治效益之道

下列十个步骤可作为高水平指导，以建构网络威胁风险管治程式，并以上页有关完善网络威胁风险管理能力的特征之探讨作为起点，了解企业的相关实力，以管理并减低当今网络威胁所构成之前所未有的风险。虽然如此，以下步骤一概不可替代由专家进行的正式、严格的信息科技安全评估。

1. 紧贴最新网络威胁的有关资讯，以及其对自身企业的潜在影响。
2. 明白到网络威胁风险智能如同传统业务智能一样重要。
3. 首席级高管人员须负责网络威胁风险管理的工作。
4. 提供足够资源，以进行企业的网络威胁风险管理工作。
5. 要求管理层就企业首要网络威胁风险管理工作，定期作出（如季度）实务报告
6. 期望高管人员能建立持续监察的方法，以助企业预测并预防网络威胁相关问题。
7. 要求内部审计部门在季度审核中，评估网络威　胁风险管理的效能。
8. 期望高管人员能紧密了解并报告网络威胁风险管理工作对企业造成之影响的量化计量。
9. 监察现有及潜在未来网络安全相关法例及法规。
10. 明白有效的网络威胁风险管理，能让公司更有信心承担若干“有意义”的风险（如采用云端技术），以追求新价值。

与企业高管团队共同探索网络威胁风险，除了有助改善该方面的风险管治，也能够创造其他价值。同时，能够引发企业董事会于高管人员就基本信息科技风险管理增加具实际帮助的讨论，并且更积极参与所有涉及信息科技风险之事务。

尾注

[1] 美国证监会公司融资监管部：〈公司融资披露指引：（二）网络安全〉：2011年10月13日

[2] 如欲获取更多资讯，请参阅〈网络威胁时代的风险智能管治 - 暗藏杀机〉

德勤《企业领导制高点》由Deloitte LLP 德勤企业领导菁英会全球调研总监Ajit Kambil博士指导下，与企业领导菁英会培训及活动规划高级经理Lori Calabro，制作，并由德勤中国企业领导菁英会总监梁小慧改编至中国版本。

德勤企业领导菁英会凭借我们的服务能力广度，交付前瞻性观点和新颖洞见，协助首席财务官应对自身角色复杂性、驱动企业价值增长以及顺应市场上瞬息万变的战略变革。

如欲了解德勤企业领导菁英会更多详情，欢迎浏览我们的网站 www.deloitte.com/cn/cfocentre

联系

聯絡我們以獲取更多相關資料

刘伟杰
全国主管合伙人 - 中国企业领导菁英会
电话：+852 2852 1015
电子邮件：danlau@deloitte.com.hk

梁小慧
总监 - 中国企业领导菁英会
电话：+852 2852 1620
电子邮件：saleung@deloitte.com.hk

HK-011SC-13

这是环保纸印刷品