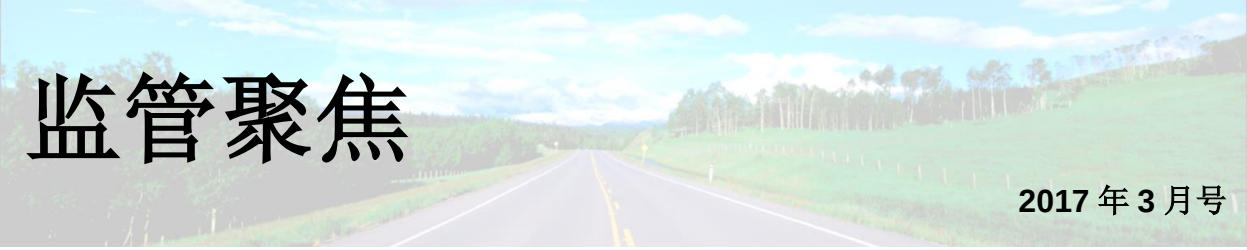

本文仅提供一般合规资讯，并不旨在构成法律或其他专业意见。

云端系统普及化 - 网络安全要注意

本文将就证监会于 2017 年 1 月 26 日发布"致所有持牌法团的通函 网络保安威胁警报"，探讨现时持牌法团的网络安全的重要性。

是天空中的云吗？

现今科技发展一日千里，不少企业都逐渐使用各种网络产品，例如谷歌网络平台与亚马逊网络服务。为追上时代的步伐，云端电脑系统更日趋普遍。根据不少统计，预计在未来几年内云端系统将普及化，并随着社会需求不断发展及改善。虽则如此，云端系统也有其风险，如资料或会外泄,监管机构对云端系统的安全性表示关注。

"云"是"网络"的一种比喻说法。云端系统是一种电子系统，用户可以随时随地将软硬件资源和信息，按需求分享至各种电子设备。用户可以通过个人电脑及智能手机等方式，将档案载入数据中心。云端服务一般可以分 3 个类别， 包括软件即服务（SaaS），平台即服务（PaaS），及基础设施即服务（IaaS）。用户可以按照自己的需求，选择云端服务设计，供应商及平台。

云端系统服务比传统电脑系统带来更多效益，因此受到不少企业的欢迎。云端服务可以提高工作灵活性，不受公司面积的限制，不受业务扩展或缩小影响, 可以降低租用或购买档案储存空间的支出，有助减低硬件及作业成本。只要有无线网络，员工就可以随时随地存取和使用公司数据与文件，提升工作效率，并消除了位置的限制。

纵使云端系统服务有不少好处，网络安全问题也受到关注。根据香港警务处，香港科技罪 案所导致的财政损失由 2014 年到 2015 年上升了 52%，而于 2015 年内香港科技罪案数字达至 6862 宗。（数据源：http://www.infosec.gov.hk/sc_chi/crime/statistics.html）其中，最主要的攻击是针对云端系统的网络攻击。

监管机构的回应

网络安全是 2016 年经济与金融界被优先关注的事项。 香港证监会于 2017 年 1 月 26 日发出「致所有持牌法团的通函网络保安威胁警报」，（http://sc.sfc.hk/gb/www.sfc.hk/edistributionWeb/

gateway/TC/circular/doc?refNo=17EC8）指一些证券经纪行被针对其网站发动的分散式阻断服务(DDoS)攻击，令其服务短暂中断，造成干扰和不便。其中，更有遭罪犯勒索的案件。证监会对此表示关注，并提醒持牌公司要提高警觉，采取相应网络保安措施应付有关风险。反分散式阻断服务机制的方法包括过滤大量及可疑的输入流量／网络攻击、制订分散式阻断服务缓解计划、与检讨网络架构和妥善配置域名系统及／或网络时间协定伺服器。

除了针对分散式阻断服务攻击之外，证监会亦对网络保安表示关注，并为持牌法团提供网络安全的监控措施。证监会于 2016 年 3 月 23 日发出 「致所有持牌法团有关网络保安的通函」，（http://sc.sfc.hk/gb/www.sfc.hk/edistributionWeb/gateway/TC/circular/doc?refNo=16EC17 ）主要关注的范畴包括：

1. 现时网络保安风险评估工作的涵盖范围不足；
2. 对服务供应商进行的网络保安风险评估不足；
3. 网络保安意识培训不足；
4. 网络保安事故管理安排不足；及
5. 数据保护方案不足。

而证监会对持牌公司提出以下建议：

- 建立稳固的管治框架，以监督网络保安管理；
- 对服务供应商实施正式的网络保安管理程序；
- 加强保安架构，以防范进阶网络攻击；
- 制定资讯保护方案，确保敏感资讯的流通得到保护；
- 加强对威胁、情报及漏洞的管理，以主动地识别及补救网络保安漏洞；
- 改善事故及危机管理程序，并在当中纳入有关最新网络攻击情境的更详尽资料；
- 制订充分的后备安排及书面应变计划，并在当中纳入最新的网络保安情况；及
- 加强使用者接达监控措施，确保使用者只在有需要知悉时方获准接达资讯。

香港金融管理局（“金管局”）亦于 2016 年 5 月 18 日在网络安全高峰会（“峰会”）上宣布推出「网络防卫计划」，旨在提高网络安全水平以维持香港国际金融中心的地位（ http://www.hkma.gov.hk/gb_chi/key-information/press-releases/2016/20160518-5.shtml ）。「网络防卫计划」由 3 个不同的计划组成，包括：

- 「网络防卫评估框架」（Cyber Resilience Assessment Framework）；
- 「专业培训计划」（Professional Development Programme）；及
- 「网络风险资讯共享平台」（Cyber Intelligence Sharing Platform）。

这三种方法是为了加强当前的网络安全系统，以及培训更多网络安全的专家。

业界回应

另类投资管理协会（Alternative Investment Management Association）于 2017 年 1 月 19 日举办了亚太地区年度论坛，一些网络安全的专家分享了关于云端资源迁移的见解，并提醒各公司必须采取预防措施，防止网络攻击。

随着云端资源迁移的增长趋势，持牌公司通常依赖外判商来管理其网络及电脑系统。专家们强调持牌公司应关注第三方责任的问题。电脑系统管理的工作外判于外面的公司时，一些公司误会以为外判意味着责任转移，但是，双方在网络受到攻击时也要对公司的客户承担责任。此外，持牌公司不应只依赖外部服务提供商，自己亦须建立资讯科技团队来监控风险和处理突发网络问题。该团队应记录任何网络安全的漏洞，并应制定应急计划来处理这些问题。

关于这一个趋势，专家们提出云端资源迁移期间的一些建议。首先，企业于使用云端系统前必须有明确目标，如处理合规问题或业务扩展；而企业们应该熟悉监管机构的规则。然后公司应该小心选择云端服务提供商，仔细考虑其服务范围，了解是否符合公司的业务需求。专家还提醒，对于计划在中国经营或已在中国经营的公司，应该确保该系统能在中国地区顺畅运作。

由于现今网络攻击的数量增加，网络保安是不可避免的重要议题。 正如香港银行学会行政总裁梁嘉丽女士在峰会上表示，在银行和金融界，网络威胁构成的风险不断上升。为了预防持牌公司因网络攻击而对社会及其客户招致损失，专家提醒持牌法团应加强其网络安全系统和了解相关监管机构的指引，并制定风险管理解决方案和网络安全措施。对于云端资源迁移，专家们建议企业应选择最适合其商业目标的服务提供商，并确保其系统的安全性。

总结

最后，持牌法团应该要加强监控和确保以下措施：

1. 严格检视及评估网络风险；
2. 矫正任何弱点；及
3. 加强网络安全措施。

如有任何有关本月监管聚焦的查询，或有任何希望我们解答的问题，请于以下链接提出：https://goo.gl/forms/gDLVThTmxGvMl4r12。

天智合规为独立顾问公司，专为亚洲的私募基金、对冲基金、基金管理公司和金融公司机构合规人员提供积极和务实的合规解决方案和建议，以帮助他们履行合规义务，并符合当地的法规要求。 天智合规团体拥有多年丰富专业经验， 包括管理及减低法规，营运及声誉风险。

我们一直以专业的合规知识，为初创对冲基金，对冲基金的基金和多策略对冲基金提供实时的合规支持和积极的建议。

通过与**天智合规**的合作，我们的客户获得可信的合规解决方案以及监管政策和程序的最新知识。透过与客户建立牢固互信的关系，作为值得信赖的顾问，我们帮助客户应对充满挑战与变化的监管环境。

联络资料:

天智合规顾问有限公司
香港中环康乐广场 8 号交易广场第 2 座 801 室
电话: (852) 3487 6903 www.complianceplus.hk

钟婉怡女士为天智合规顾问有限公司董事。钟女士在资产管理行业、共同基金及对冲基金的法律及监管事宜上拥有超过 15 年的经验。在此之前，钟女士为主要资产管理集团的法律及合规部主管，并负责相关管理业务的合规监督和法律问题。

欢迎致电+852-3487 6333 或电邮 jchung@complianceplus.hk 联系钟婉怡女士。

完

© 天智合规顾问有限公司。保留所有权利。最后更新于 2017 年 3 月