CHARLTONS
易周律师行

通讯 - 香港法律 2020年5月

证监会就2019冠状病毒大流行 (COVID-19) 期间遥距工作安排的网络保安风险管理向持牌法团发出指引

2020年4月29日，证券及期货事务监察委员会（证监会）发出了《致持牌法团的通函与遥距工作安排的网络保安风险管理》[1]（证监会网络保安风险通函），提醒证监会持牌法团须评估其操作能力，及实施适当的措施以管理与遥距工作安排相关的网络保安风险。证监会是鉴于新冠病毒大流行期间愈来愈多公司采用遥距工作安排的情况而发出该指引。

透过遥距工作安排，雇员可以从办事处以外的地点接达证监会持牌法团的内部网络和系统。遥距工作安排还可以让员工透过视像会议举行会议。证监会网络保安风险通函就监控措施及程序列举了多个例子（非详尽无遗），以协助证监会持牌法团保护内部网络及数据。

《证券及期货事务监察委员会持牌人或注册人操守准则》第4.3段规定，持牌法团须设有妥善的内部监控程序、财政资源及操作能力，而按照合理的预期，这些程序和能力足以保障其运作、客户及其他持牌人或注册人，以免其受偷窃、欺诈或不诚实的行为、专业上的失当行为或不作为而招致财政损失。因此持牌法团须实施并维持其视为适当且与其业务规模及复杂程度相称的监控措施及程序。

遥距接达证监会持牌法团的内部网络

员工一般透过虚拟私有网络（Virtual Private Network，简称VPN）软件接达证监会持牌法团的内部网络。VPN软件透过互联网提供加密连接，从而使得雇员能够遥距接达内部网络并确保敏感数据在传输过程中得到保护。证监会网络保安风险通函中提到近期某持牌法团所汇报的一宗网络保安事故，并特别指出网络罪犯如何利用VPN的已知缺陷入侵证监会持牌法团的内部网络，存取客户数据及发出未经授权而转移资金的指示。

纾减网络保安风险的监控措施及程序

证监会网络保安风险通函列出以下用以纾减遥距接达网络保安风险的监控措施及程序：

1 证监会。2020年4月29日。《致持牌法团的通函-与遥距工作安排相关的网络保安风险管理》。载列网页：https://sc.sfc.hk/gb/www.sfc.hk/edistributionWeb/gateway/TC/circular/intermediaries/supervision/doc?refNo=20EC37

(i) 实施稳健的VPN解决方案，藉以提供强效的加密程式及两重或以上的防护，以保护在遥距接达装置与持牌法团内部网络之间传输的数据；

(ii) 使用多个VPN伺服器以提供额外保障；

(iii) 及时监察、评估及执行VPN软件提供者发布的保安修补程式或修正程式。多个资讯科技保安专业人士已对以下事项表示关注：使用存在未修补漏洞VPN软件的组织可能容易被黑客入侵，危害组织内部网络；

(iv) 规定雇员、代理及服务提供者须使用难以破解的登入密码来进行遥距接达，及实施双重认证，尤其是在接达特权账户及敏感数据时；

(v) 避免向第三方人士授出常设或永久接达权，及只容许系统供应商在预设的时段内接达特定的系统；

(vi) 实施不同级别的遥距接达，例如确保持牌法团所提供的电脑和流动装置具有比雇员私人拥有的装置更佳的操作能力；

(vii) 实施保安监控措施，以防止有人在未经授权的情况下为证监会持牌法团供应的电脑和装置安装硬件和软件；及

(viii) 实施稳健的网络隔离措施，以根据关键程度来分隔系统伺服器及数据库，从而加强保护关键和敏感数据，例如客户个人资料。

证监会持牌法团使用视像会议

与视像会议相关的保安问题时有报道。证监会建议持牌法团采用以下监控措施及程序以降低出现安全漏洞及泄露关键或敏感数据的风险：

(i) 在使用视像会议平台之前，审查其保安特点；

(ii) 规定参与者须登记方可出席视像会议；

(iii) 透过确认使用者的电邮地址或利用“等候室”功能（让视像会议主持人可只准许获授权的参与者加入会议）等方式，只准许经认证及获授权的使用者加入视像会议；

(iv) 使用随机的会议编码而非个人会议编码举行视像会议；

(v) 透过视像会议软件或其他适当途径（例如工作电邮）向参与者发送邀请，同时不在社交媒体平台分享邀请；

(vi) 在视像会议平台上启用密码保护功能；

(vii) 于所有参与者加入后闭锁会议；及

(viii) 确保使用最近期版本的视像会议软件，并安装最新的保安修补程式。

其他遥距工作安排网络保安风险措施

证监会还推荐证监会持牌法团采用以下措施，藉以提升操作能力，及监察各项遥距工作安排机制：

(i) 系统能力：评估现有的资讯科技系统，软件（例如遥距电脑装置，网络频宽及软件许可证）及硬件（例如手提电脑及流动装置）就支援遥距工作安排是否足够，并对其加以改进；

(ii) 监察及事故处理：制定监察机制，以侦测未经授权而接达内部网络及系统的情况，例如检视未经授权的接达尝试，及侦测使用未经批准的应用程式的情况。设立并维持有效的事故管理与汇报机制；及

(iii) 网络保安培训及警示：向所有内部系统使用者提供适

当的网络保安培训，及定期向客户发出提示和警示，例如仿冒诈骗[2]及勒索软件[3]方面的网络保安威胁及趋势事宜，以及使用安全的无线网络来接达内部网络和视像会议平台。

鉴于新冠病毒大流行期间居家办公安排的兴起，遥距工作安排可能会越来越普遍，证监会持牌法团应评估及检视其网络保安监控措施以确保其符合适用法律法规的要求。

证监会邀请持牌法团就本通函中提及事项的任何疑问联络个案主任。

2 仿冒诈骗是指黑客试图诱骗使用者犯错，例如点击会下载恶意程式的连接，或将他们导引至欺诈网站。

3 勒索软件是对文件进行加密使得文件无法打开并要求支付费用才给予解密的一种恶意程式。

CHARLTONS
易周律师行

Award winning Hong Kong law firm

此通讯仅为提供相关资料信息之用，其内容并不构成法律建议及个案的法律分析。

此通讯的发送并不是为了在易周律师行与用户或浏览者之间建立一种律师与客户之关系。

易周律师行并不对可从互联网获得的任何第三方内容负责。

如果您不希望收到该法讯，请电邮 unsubscribe@charltonslaw.com 告知我们

香港皇后大道东43-59号
东美中心12楼
电话: 852 2905 7888
传真: 852 2854 9596
www.charltonslaw.com