一图看懂：远程和移动办公安全

（来源：普华永道中国公众号，2020-04-07）

疫情当前，远程办公成为兼顾员工健康和业务运转的最佳方式。但同时在远程办公过程中的信息和数据安全应引起企业和员工的高度重视。远程办公在开启了方便之门的同时，极大的复杂化了业务系统、重要数据和办公网络的操作场景，进一步扩大了信息安全风险。企业需要从技术架构、数据管理和员工行为等多维度，多领域的系统化统筹，以实现效率与安全的统筹兼顾。面临纷繁复杂的远程办公场景，我们用**一张图读懂远程办公安全要点，一句话理解数据安全保护重点。**

在远程办公操作安全保障的基础上，针对企业的数据安全，尤其是涉及企业核心商业价值的重要数据，还应围绕数据进行进一步的安全防护。在这里我们用一句话总结远程办公中数据安全的保护要点：**控源头、限接触、勤监控、早阻断。**

远程数据产生和存储风险

○ 风险场景：远程办公环境下，企业重要数据的产生和存储更加分散，同时数据访问和接入途径更加多样，由于办公需要，数据访问权限需要进步一扩展等，这些均导致数据在生产和存储过程中泄露风险极大提升。

○ 应对提示：控源头，数据分级管理，严控数据源头。

在远程办公场景下，需重点管控两个数据源头。

一是企业云端或服务器端，需要对数据进行分类分级管控，对于高级别的重要数据，应严格限制远程访问的账户、访问权限及远程接入方式。对于访问账户，建议在进行远程办公同时，整理和排查当前账户的合法性，及时清除非法或失效账户。同时关注系统授权的合理性，对需要临时授权的账户，进行严格的授权审批，并在工作完成后及时收回权限。对于远程接入方式，应采用企业 VPN 接入办公。如不

具备 VPN 接入条件，应采用 HTTPS 对访问通道进行加密，同时采用双因素授权的方式进行远程登陆。有条件的企业，我们建议对于重要数据采取数据不离线的工作方式保障数据安全,远程办公所有的操作的数据均在云端和服务端存储，禁止数据传下载至移动办公终端。

二是移动办公终端，应严格限制移动终端的使用，禁止使用未经企业注册或登记的个人移动设备办公。同时，对移动办公终端所产生的数据进行加密存储，并在数据传输时，将加密数据和加密密码采用不同方式分别传输。

远程复杂网络环境风险

○ 风险场景：远程办公不同于集中办公，其所处的网络环境更加复杂，4G/5G 网络热点、家用 WIFI、公用 WIFI 等，接入网络变得不可信任，可能导致利用钓鱼网路的中间人窃取数据。终端接入种类多样，应用软件的使用更加灵活，企业软件、个人软件、通用即时通信软件、网络邮箱、网盘和云盘等应用程序的使用，使得数据更多的暴露在不可信的环境中，导致数据泄露风险。

○ 应对提示：限接触，保障环境可信，限制用户接触。

在控制数据产生存储源头的基础上，还需要对数据传输和使用进行进一步管控。对于云端和移动终端，以及移动终端之间的数据交互，应对数据通信全链路进行 HTTPS 加密，防止数据在传输中泄露或被窃取。另外需要特别注意的是，对于传输数据的邮件或及时通信工具，需要严格加以限制，应使用企业邮箱和专用通讯工具进行数据传输，禁用公共邮箱和通用及时通信工具传输企业数据。对于移动终端而言，还需要注意接入的网络热点和 WIFI 安全，不要接入未知的网络热点和 WIFI 处理办公数据，尤其是无需密码就可直接登陆的网络，谨防

非法网络窃取数据。

远程用户访问和操作风险

○ 风险场景：在远程办公场景下，用户需要远程访问系统并处理或下载数据，用户身份和访问行为都变得更加不可信，假冒合法用户访问，用户越权访问，批量数据下载、高敏感数据的修改和删除等异常访问和操作等攻击行为，可能导致重要数据的大批量泄露或不可用。

○ 应对提示：勤监控，丰富监控手段，提升监控频率。

企业应考虑对数据生命周期进行全面监控。在云端和服务端，重点监控访问系统的用户行为，包括用户身份、授权范围、访问时间、访问方式、访问内容、访问频次、操作行为和数据传输内容等信息，尤其需要关注短时内的异地登陆，多次的用户登陆失败后的登陆成功，用户登陆后短时间的系统各页面间的高频访问，用户登录后的数据批量下载或修改等行为；另外还需重点监控系统接口的数据传输情况，包括数据类型、数据传输量、传输频次等。在移动办公终端，重点监控用户对重要数据的操作行为，包括数据存储位置，通讯工具传输行为，数据 U 盘拷贝等。另外还需提升对用户密码强度和修订次数的监控，建议在远程办公期间，加密用户密码复杂度的要求，同时增加更换密码频率，进一步缩短密码有效期。通过对数据生命周期重点场景的监控，及时发现和纠正违规行为，提升数据保护能力。

数据泄漏的应急管理

○ 风险场景：无论如何防护，远程办公环境下的数据的生产、存储、传输和使用，都会相比于集中式办公环境进一步增大数据安全风险。因此企业需要未雨绸缪，提前考虑体系化的预防和应急管理，

避免应对不当导致损失的进一步扩大。

○ 应对提示：早阻断，及时修复漏洞，提前部署预案。

一旦发现可能的数据安全风险问题，需要及时阻断以降低企业损失。具体措施建议重点关注三个领域。一是系统安全漏洞的加固和修复。在远程办公环境下，需要加强对服务器操作系统、中间件、数据库和相关开源组件等安全漏洞的扫描频次，对于服务端和移动终端出现的安全漏洞，需要及时进行修复和加固，避免黑客利用漏洞远程窃取数据；二是异常操作行为的阻断，针对上一小节中的异常行为，从管理和技术层面加强建设，针对发现的风险及时告警和阻断；三是数据泄露后的应急处置，企业需要提前制定应急预案，尤其是远程办公环境下，数据泄露、数据窃取、数据误操作等风险的场景化预案，对问题进行及时响应和处置。

数据安全保护如同疫情防控，需要企业和员工充分重视并积极行动，“控源头、限接触、勤监控、早阻断”发现问题及时处置，必要时寻求第三方专业机构或监管机构的帮助。

在这个特殊的时期，普华永道安全团队希望向我们的合作伙伴乃至社会公众强调疫情下面临的数据安全和网络安全风险，进而更加稳健地恢复工作及生活，携手并进，共渡难关。

原文链接：https://mp.weixin.qq.com/s/D5IgeTbOKQQme8teKXx8aQ ，转载请注明。