风险应对有道 驱动后量子时代的数据保护

居家办公、虚拟银行和在线购物的出现提高了人们对数字世界的依赖度，随之而来的是日趋激化的量子霸权争夺战。层出不穷的新兴技术，使企业的各类操作系统逐渐难以抵御来自量子计算机的网络攻击。

以下问答中，普华永道中国数字化办公室合伙人季瑞华及网络安全与隐私保护服务合伙人冼嘉乐均强调：**企业应即刻开始为后量子时代的数据保护做准备**。

问 量子计算将带来哪些风险？对信息安全有哪些影响？

答 传统或经典计算目前已经发展到了第4代。19世纪初以来，计算机的技术进步从未间断，从最初的真空管、晶体管和集成电路，到现在的微处理器，不一而足。但所有这些技术发展的基础都是电路在给定时间在单一状态（开通“1”或关断“0”）下的使用。

而量子计算的基础是量子力学现象，它能够以多种状态出现。经典计算机以“位”（用1或0表示）为单位保存和处理数据，而量子计算机则以“量子比特”（其可为1或0，并处于1和0的叠加状态）为单位保存和处理数据。这一特性使量子计算机具备了经典计算机所不具备的功用。

量子计算对信息安全的影响是不难理解的。现在的所有机密、有价值数字信息和资产都通过使用加密技术来保护。即便使用功能更强大的计算机，要用现在的计算技术找到安全漏洞也需要花费数万亿年。

而量子计算出现后，其将大幅缩短找到并突破安全漏洞所需的时间，从而将现在用加密技术保护的所有资产置于风险之下。

问 哪些行业更易受量子威胁的影响？

答

日常生活的方方面面都依赖加密技术来保护重要信息资产，例如：

- 电信网络是加密的，选择在家办公时，人们与办公系统之间的通信通道也是加密的。
- 信用卡和付款详情、银行账户，甚至是加密资产的数字钱包也都依赖于加密技术。
- 各类敏感和机密信息，从健康记录到商业合同，都通过同一套加密技术保护。

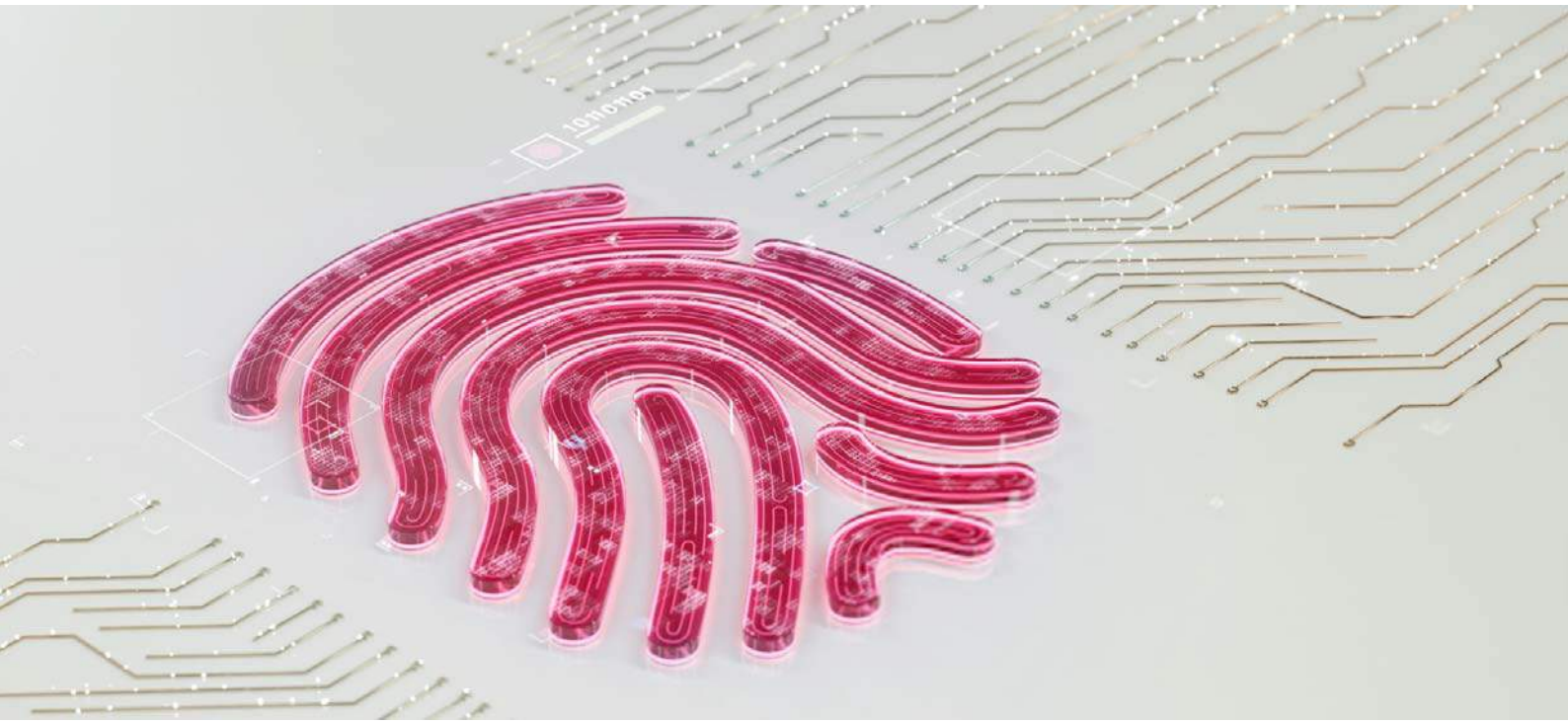
因此，量子计算的影响是无处不在的，任何行业部门都不例外。部分行业或部门还因为较多地依赖于加密技术而将遭受更多的量子威胁，如电信、银行与金融、医疗健康、认证机构，以及一些新兴的数字资产或分散金融领域。

问 什么是后量子密码（PQC）？后量子密码为何很重要？

答

后量子密码，有时也称为量子安全或量子抵抗密码，是密码算法领域的一个术语，设计用于当今的经典计算机，但具备抵御经典计算机和量子计算机的潜在攻击能力。

之所以需要部署这一新一代的加密方案，是因为现在所使用的很多系统内均深入部署了各类加密技术，且很多这些加密技术之间还是相互联系的。要了解当前正在使用何种加密工具，并在确保互操作性的前提下将其替换为新的加密工具，这一过程将可能耗时颇巨。考虑到量子计算技术的高速发展，明智的做法是提前规划，以应对这一新的安全威胁。



问 后量子加密方案是否有完备的行业标准可支持商业应用？

答 作为世界领先的技术标准制定者之一，美国国家科技学会（NIST）指出量子计算机可能带来的潜在威胁，因其用时二十年才部署完成现在的公钥基础设施，可满足人们当前的通信和安全需求。NIST的结论是：“或许尚无法准确估计量子计算时代的确切到来时间，但必须从现在开始做准备，确保人们的信息安全系统能够抵御量子计算威胁。”

2016年12月发起了一场为后量子加密算法提名的竞赛。完成了前两轮的竞赛后，第三轮竞赛的候选人（包括7名决赛选手和8名替补选手）已于2020年7月公布[https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions]。根据该竞赛的时间计划，预计标准的草案将于2022-2024年期间发布。

换言之，后量子加密算法的最终行业标准至少要两年之后才会出台。

问 既然还没有相关标准，那为何需要企业即刻开始准备应对量子风险呢？

答 以此次疫情为例，没有疫苗并不意味着什么都不做。网络安全领域也一样，采用相同的方法来抗击计算机病毒：除配备防病毒工具之外，还建立了一套强大的预防性控制措施，从提高意识到采取一系列预防和检测措施，以最大程度降低病毒攻击的风险。

现在，加密方案的广泛使用意味着，当量子计算技术的进步实质威胁到当前使用的所有公钥加密方案时，对人们有价值的所有信息资产都将面临风险。加密模块（通常存在于应用程序和技术基础设施中）的升级或修改需要严格规划和协调，更何况这还是一个高度专业化的领域，需要主题专家的投入和参与。需要严格规划和协调，更不用说这还是一个高度专业化的领域，需要主题专家的投入和参与。

因此，企业应将后量子安全纳入其总体网络安全战略之中。企业高管和董事会都应重视这一点。事实上，Visa、JP Morgan Chase、Google等公司都已经率先开始准备应对这一潜在风险。监管机构和政府也应时刻关注此类新出现的风险。在后量子加密标准发布前，需要先提供必要监管指导的可能性较大。

问 企业现在可以开始做哪些工作来准备应对量子挑战呢？

答

1. 增强对这一潜在威胁的认识，了解为何需要现在采取措施。
2. 制定相关流程以识别对企业至关重要的数据资产，编制此类资产清单，并确定保护此类资产的时间长度。
3. 关注后量子加密标准的制定进度，了解各类密码方案的用途，确保企业可在标准出台后随时采用这些标准。

考虑系统间的相互连接，上述标准的采用可能还需要与同行或行业机构协调，甚至可能还需要接受监管机构的指导。

普华永道将继续跟踪后量子加密标准的制度进度，在这一重要问题上与主题专家协作，并计划与客户和监管机构分享更多见解和良好实践，探索适用的技术方案，确保现在使用的安全基础设施的持续有效性。

联系我们

季瑞华
合伙人
数字化办公室
william.gee@cn.pwc.com

冼嘉乐
合伙人
网络安全与隐私保护服务
samuel.sinn@cn.pwc.com