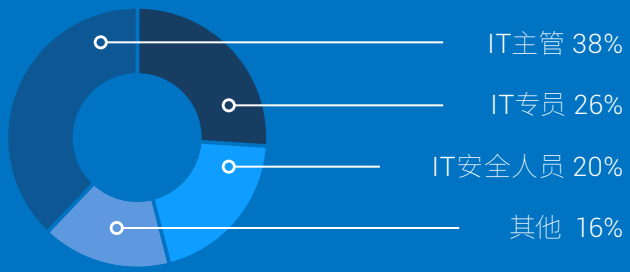
digicert®

量子的前景与风险：2019 年度 DIGICERT 后量子加密调研

方法论

DigiCert委托德克萨斯州达拉斯的ReRez Research公司进行调研，调研对象是400家企业的IT专业人员，这些企业位于美国、德国和日本，员工人数不少于1000人。

受访者被分为IT主管、IT安全经理与IT专员。



本次调研聚焦于四个重要垂直行业：

金融业　医疗业　交通运输业　工业

量子的前景与风险

IBM 2019 年 1 月推出了全球第一台基于电路的商用量子计算机 IBM Q System One。尽管实现量子计算机的全面商用化依然任重道远，但是量子计算机很有可能解决目前的数字计算机无法解决的诸多问题，这让许多人感到振奋。机器学习、医学与粒子物理学是量子计算有望颠覆的几个重点领域。

然而量子计算的前景并非全都有益无害。美国国家标准与技术研究院（NIST）与许多其他领军者预测，将来的量子计算机很可能在未来十年内破解目前最复杂的加密算法，从而引发深远的安全问题。

在此之前，行业必须开发出新的加密算法——即能够抵御量子计算威胁的算法。这些算法被称为后量子加密（PQC）。不过PQC并不是答案的全部。

以物联网为例。PQC是行业用以描述能够抵御量子计算机攻击的算法的术语。然而，如果企业的物联网设备与应用程序生命周期比较长，则首批量子计算机将威胁到它们在未来的运行，这些曾经安全的产品或将成为负债。配备传感器、车载计算机并联网化的汽车就是一个例子。如果现在在制造这些设备/产品时没有采取量子安全策略，那么它们就可能在未来遭受攻击。

为了实现充分的保护，企业必须从现在就开始应对量子计算威胁。然而企业应该怎样进行准备？企业应该采取什么行动？企业对PQC的了解有多少？

为了探讨这些问题以及其他的PQC问题，DigiCert委托 ReRez Research 公司进行了2019 年度 PQC 调研，DigiCert 是全球领先的 TLS/SSL 证书以及其他用于网站、企业应用程序与物联网的数字证书供应商。调研结果显示，行业从业者应当行动起来，共同应对量子计算所带来的挑战。

对 PQC 普遍有了解，但存在初期困惑

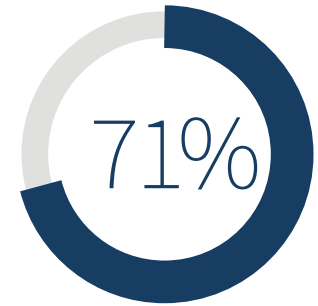
企业的 IT 人员基本上都非常熟悉 PQC 这一术语。当被问到这个问题时，每十个人中就有七个人表示他们对 PQC “比较”了解到“完全”了解，但实际情况并不完全如此。之后我们问了一个问题，这个问题旨在测试他们是否真正了解PQC的含义。只有不到三分之二的人知道 PQC 的正确内涵。

更明显的是，有 59% 的人表示现在正在部署混合型 (PQC+RSA/ECC) 证书——然而这是不可能的，因为现在的 PQC 证书仅供早期测试之用。

不过这并不奇怪，PQC 是新生事物，大家仍然在学习其含义及其应对方式。这很类似于 2012年的一项调研结果，当时有超过半数的受访者认为“暴风雨天气”会影响“云计算”。 1 尽管他们很困惑，但他们仍然知道云计算。不过这种困惑并没有持续很长时间。如今，全球云计算的市场规模已经达到了 2140 亿美元。

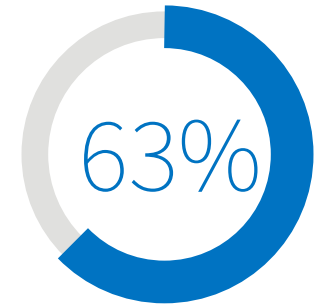
显而易见的是，许多人知道量子计算，而且量子计算正在影响着他们现在和未来的思维方式。本次调研进一步探索了安全专业人员计划如何应对量子计算对加密的威胁。

“我们仍处于初期探讨阶段，因为我们不是唯一受影响的企业。我们正在与第三方合作伙伴及供应商探讨，如何积极主动地增强我 们的安全性。 量子加密是我们正在研究的课题之一。”一家金融服务公司的IT安全经理表示。



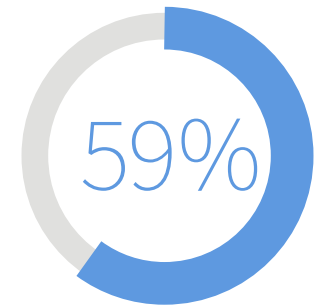
表示“比较了解到完全了解”

然而……



选对了 PQC 的内涵描述

而且……

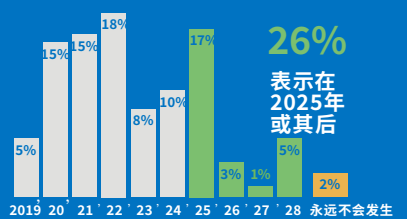


表示他们现在正在部署混合型 (PQC+RSA/ECC) 证书

1. 51%的受访者认为暴风雨天气会影响“云计算”—— Business Insider，2012年8月30日

何时

量子计算将于何时有能力破解现有的加密算法?



26%
表示在2025年或其后

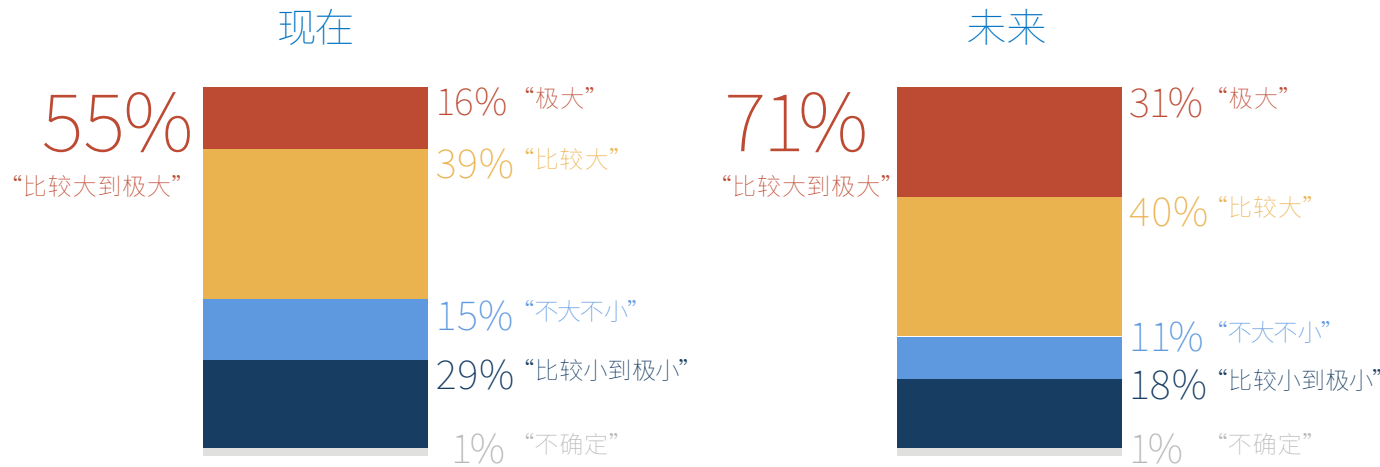
几乎每个人都认为，当威胁成为现实之际他们仍将在各自的公司工作

每10个人中有8个人

表示了解量子安全的安全实是比较重要到极为重要的

量子计算威胁真实存在且快速逼近

尽管有些困惑，但IT从业人员还是清晰地注意到了量子计算对加密的威胁。略超过一半（55%）的受访者表示，目前量子计算是“比较大”到“极大”的威胁，71%的受访者表示，在未来量子计算将会是“比较大”到“极大”的威胁。

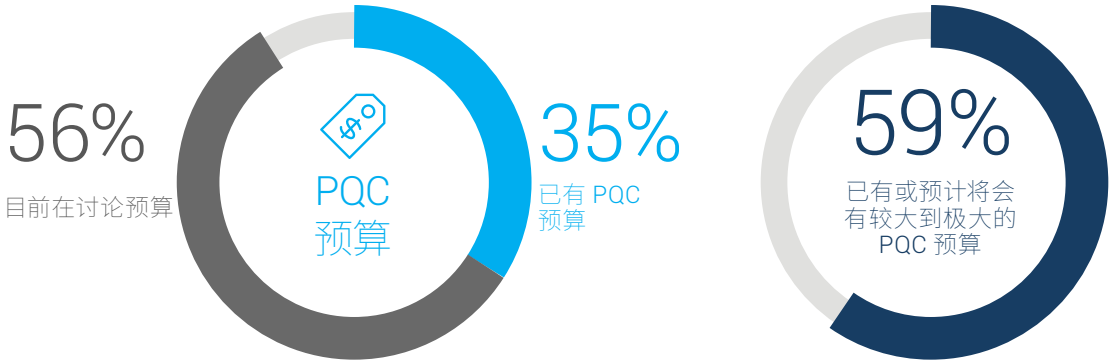


确切的说，从 PQC 的角度而言，IT 人员认为的未来是什么时候呢? 未来似乎并不太远。对于何时需要 PQC 来抵御量子计算机所造成的安全威胁而言，中值预测是 2022 年。实际上，只有四分之一（26%）的人表示2025年或其后才需要 用到 PQC。

由于威胁可被明显感知，而且时间期限紧迫，因此毫不奇怪的是，大多数（83%）受访者表示对于 IT 人员而言，学习和了解量子安全的安全实践非常重要。除了学习了解 PQC 之外，IT人员还需要做什么准备?

为 PQC 做准备

企业正在开始为 PQC 做准备，有三分之一的受访者表示他们已有 PQC 预算，另有 56% 的受访者表示他们正在为制定 PQC 预算而努力。这些预算有多大？大多数受访企业 (59%) 表示其 PQC 预算“比较”大到“极”大。 资金被分配给咨询、产品与工作人员。



就具体行动而言，毫无疑问“监测”是 IT 从业者目前所采用的首要策略；接下来是了解其组织的加密敏捷性水平。这反映了人们充分认识到在有必要转换 PQC 证书的时候，应当转换得快速而高效。

五大头部 IT 策略中的其他几项分别是了解组织当前的风险水平、积累PQC相关知识，以及开发TLS最佳实践。

五大减轻策略

1. **监测**
2. **加密敏捷性**
   了解组织的加密敏捷性水平
3. **风险**
   了解组织当前的风险水平与可接受的风险
4. **积累知识**
   积累关于 PQC 及其影响的知识
5. **最佳实践**
   开发组织内部的TLS最佳实践

PQC 之战的特征

IT 人员很清楚他们所面临的来源于量子计算的加密风险。首先，IT 人员担心应对未来的量子计算威胁/攻击的成本将一发不可收拾。其次，他们担心按照现行标准进行安全加密的数据将在未来的量子时代变得易于破解。这意味着如果数据现在失窃，那么数据目前可能是安全的，但是一旦量子计算机得以应用，这些数据就会变得岌岌可危。

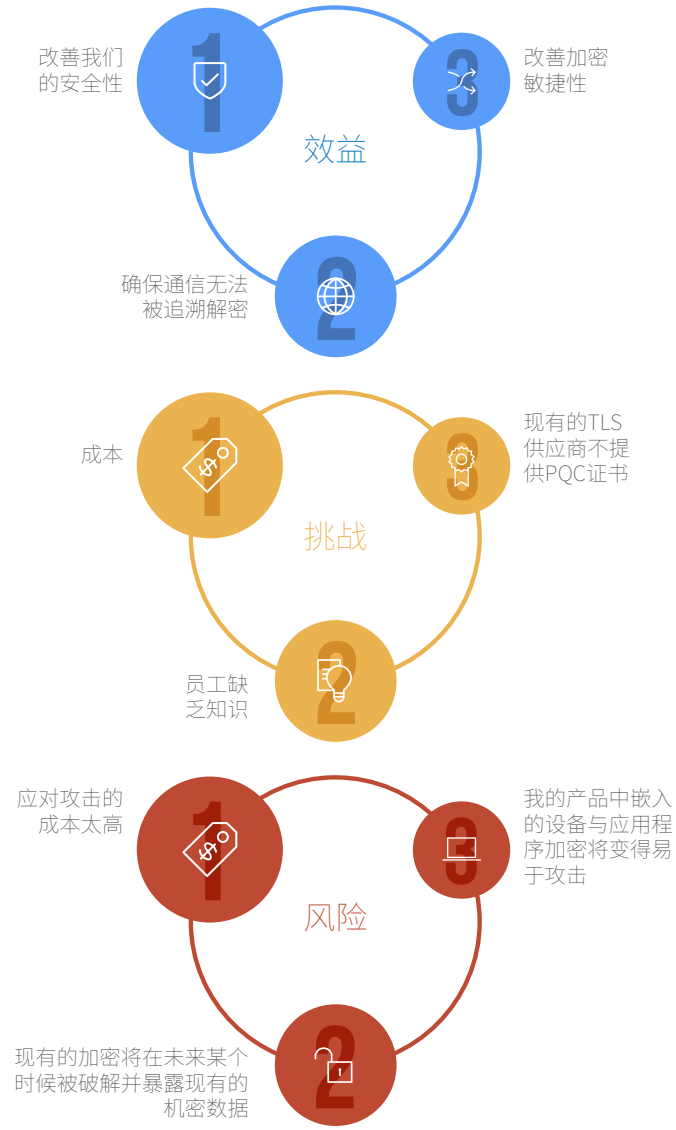
对于物联网设备也有类似的担忧。使用当今最好的加密技术进行设计意味着这些设备可以抵御目前的攻击，但容易被未来的量子攻破。对于汽车或自动取款机等长寿命产品而言，这会成为一个大问题。

因此，IT 人员致力于进行量子之战。为什么？赢得这场战役的预期效益包括改善公司的安全性，确保通信获得保护不会在未来被解密，以及最终改善加密敏捷性。

终极效益——加密敏捷性——即是在策略上承认，加密技术的世界将在未来发生快速变化，而且企业要能够在使其网络不中断的情况下迅速用新算法替换旧算法。

尽管这些效益值得争取，但是IT人员在这场量子之战中也认识到了一些挑战。根据受访者的说法，最大的挑战是成本。员工普遍缺乏有关量子攻击及其防御方法的知识，使这一情况更为恶化。最后，受访者提及的一个普遍担忧是，现有的 TLS 供应商可能无法及时提供足够的 PQC 证书。

总的来说，IT 人员对于其所面临的挑战持现实态度。实际上，近五分之二的受访者表示，升级加密技术以抵御量子计算的攻击比较困难到极为困难。



“在将来，它将会发生，而届时我们必须要为其做好准备。”一家医疗服务公司的IT经理表示。

DigiCert建议

量子计算是将会决定公司未来的三项关键技术之一。

然而量子技术的前景却因其对加密技术所造成的威胁而受到影响。对于已经准备开始规划其策略，以便在未来的量子时代背景下确保安全的企业，全球网络加密技术的领军企业 DigiCert 提供以下三大建议：

风险

了解贵公司的风险并建立量子加密期限模型

能力

了解加密敏捷性在组织的重要性，并将其确立为核心实践

最佳实践

与领先的供应商合作，确立数字证书最佳实践，并确保他们能跟进PQC行业发展前沿，帮助组织的产品和解决方案保持行业领先地位。变化往往不会在一夜间发生，组织不能一直等待，而应当立即解决其加密敏捷性问题。

版权所有©2019 DigiCert, Inc.。保留所有权利。DigiCert及其徽标是DigiCert，Inc.的注册商标。赛门铁克与诺顿及其徽标是根据赛门铁克公司的许可所使用的商标。其他名称可能是其各自所有者的商标。

digicert®

联系我们

DigiCert, inc.
2801 North Thanksgiving
Way Suite 500
Lehi, Utah 84043

1.800.896.7973
www.digicert.com

DigiCert 是全球首屈一指的高保障度数字证书提供商 —— 为新兴的物联网市场提供值得信赖的SSL、专用与managed PKI 部署及设备证书。公司建立15 年来，我们致力于互联网提供身份验证找到更优化的数字证书。—种为互联网提供身份验证的更好的方式，并根据我们的客户需求量身定制更好的解决方案。如今，赛门铁克的经验与人才的加入，让我们在原有的创新基础上如虎添翼，提升了我们的行业领导力，强化了我们在身份与数字交互领域中被信任水平。