digicert®

Quantum's Promise and Peril

DigiCert post quantum crypto survey

SURVEY REPORT

Quantum's Promise and Peril

IBM introduced the world's first circuit-based commercial quantum computer, the IBM Q System One, in January 2019. While full commercial availability of quantum computers is still a ways off, many are excited about quantum computing's promise to address many problems simply too difficult for today's digital computers to tackle. Machine learning, medical sciences and particle physics are prime examples of fields that quantum computing is expected to disrupt.

But not all of quantum computing's promise is for good. NIST and many other leaders predict that future quantum computers will—likely within the next decade—be able to break today's most sophisticated encryption algorithms, leading to profound security issues.

Before that time, the industry will have to develop new cryptographic algorithms—ones that are able to withstand quantum computing threats. These algorithms are referred to as Post Quantum Cryptography (PQC). But PQC isn't the full answer.

Take IoT, for example. PQC is the term the industry uses to describe algorithms that will be able to withstand attacks by quantum computers. But business with IoT devices and applications with long life cycles may have their products operating out in the world after the first quantum computers become a threat, and thus these once-safe products would become a liability. An example would be automobiles with sensors, onboard computers, and connection to the internet. If quantum-safe strategies are not put in place today when manufacturing these devices/products, they could be breached in the future.

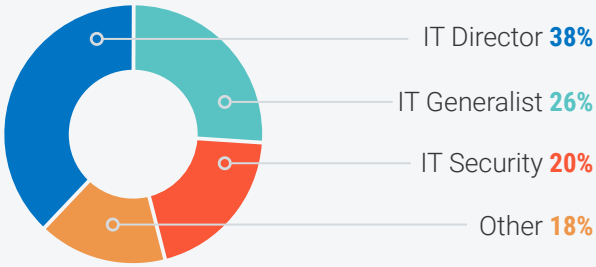
To be fully protected, businesses must begin to address the quantum computing threat today. But how should they prepare? And what should they do? How much do enterprises even know about PQC?

To explore these and other PQC questions, DigiCert, the world's leading provider of TLS/SSL and other digital certificates for websites, enterprise applications and IoT, commissioned the 2019 PQC Survey. The results represent a call to action for the industry.

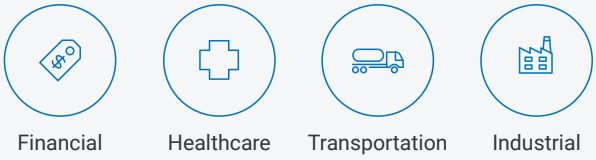
Methodology

DigiCert commissioned ReRez Research, of Dallas, Texas, to survey IT professionals within 400 enterprises of one thousand or more employees in the US, Germany and Japan.

The respondents were split between IT directors, IT security managers and IT generalists.



The survey focused on four key industries:



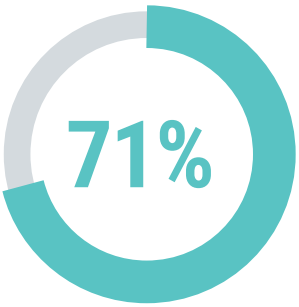
Broad awareness of PQC, but early stage confusion

Enterprise IT is generally well aware of the term PQC. When asked, seven in ten say they are "somewhat" to "completely" aware of PQC, but that's not the entire story. We followed up with a question designed to test if they truly understood what PQC means. Less than two-thirds knew the correct definition.

Even more telling, 59 percent claim to currently be deploying hybrid (PQC + RSA/ECC) certificates, something that is unlikely as PQC certificates availability is limited to early testing situations.

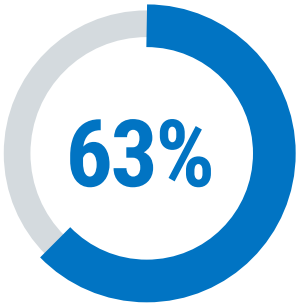
Yet this isn't surprising, as PQC is new and people are still learning about what it means and how to react. This is much like the 2012 survey that found more than half of people believed "stormy weather" would affect "cloud computing."1 While they were clearly confused, they were aware of cloud computing and their confusion didn't last long. Today the cloud computing market is a $214 billion market worldwide.

What is clear is that quantum computing is on the minds of many and is impacting their current and future thinking. This study explores further how security professionals plan to deal with the threats of quantum computing to encryption.



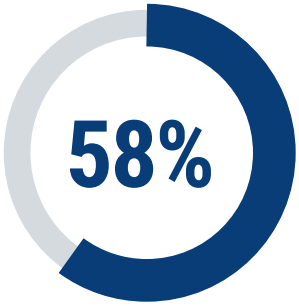
say "somewhat to completely aware"

yet...



chose the correct description of what is PQC

and...



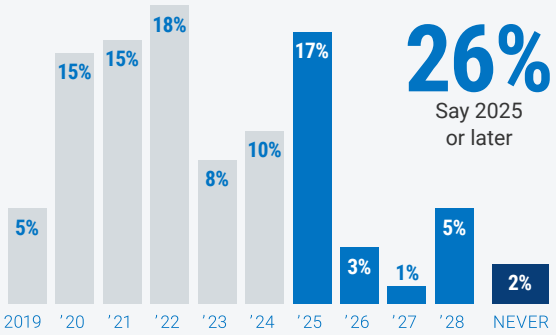
say they are currently deploying hybrid (PQC + RSA/ECC) certs

"We're still in the early discussion phases because we're not the only ones who are affected. We are talking with third-party partners and vendors on how we can be proactive and beef up our security. And quantum cryptology is one of the topics that we are looking at," — said an IT Security Manager at a financial services company..

1. 51% Of People Think Stormy Weather Affects 'Cloud Computing' – Business Insider, August 30, 2012

When

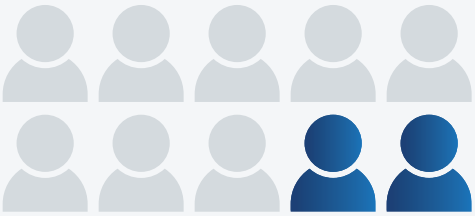
When will quantum computing advance to able to crack existing cryptographic algorithms?



26%
Say 2025 or later

Nearly everyone feels they will still be working at their company when the threat becomes real

8 out of 10



Say it is somewhat to extremely important for IT to learn about quantum-safe security practices

The quantum computing threat is real and quickly approaching

Despite some confusion, IT clearly sees the threat quantum computing poses to cryptography. Slightly more than half (55 percent) say quantum computing is a "somewhat" to "extremely" large threat today, with 71 percent saying it will be a "somewhat" to "extremely" large threat in the future.

Today

55%
"Somewhat to extremely large"

16%
39% "Somewhat large"
15% "Neither small nor large"
29% "Somewhat to extremely small"
1% "Not sure"

In the future

71%
"Somewhat to extremely large"

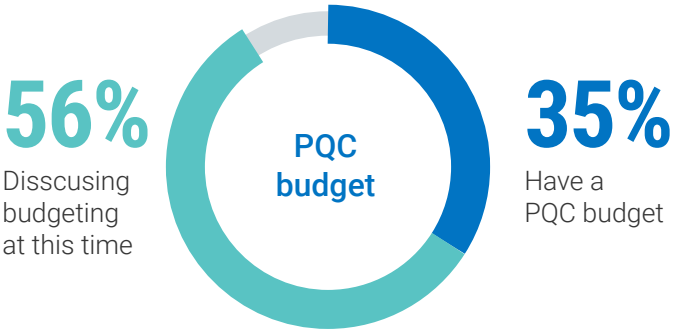
31% "Extremely large"
40% "Somewhat large"
11% "Neither small nor large"
18% "Somewhat to extremely small"
1% "Not sure"

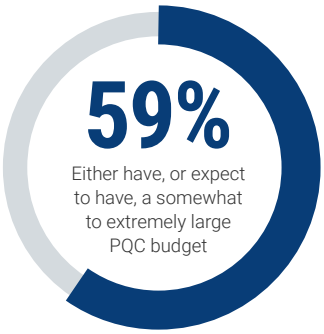
And what, precisely, does IT believe defines "future" when it comes to PQC? Not too far away, it seems. The median prediction for when PQC would be required to combat the security threat posed by quantum computers was 2022. In fact, just one in four (26 percent) say PQC will take until 2025 or beyond to arrive.

With the threat so clearly felt, and the time horizon so short, it is no surprise that most (83 percent) say it is important for IT to learn about quantum-safe security practices. Beyond learning about PQC, what else is IT doing to prepare?

Preparing for PQC

Enterprises are beginning to prepare for PQC, with a third reporting they have a PQC budget and another 56 percent working on establishing such a budget. And the size of these budgets? Most enterprises surveyed (59 percent) say their PQC budget will be "somewhat" to "extremely" large. The funds are divided between consultants, products and staff.





Top five mitigation strategies

1. **Monitoring**
2. **Crypto-agility**
   Understanding your level of crypto-agility
3. **Risk**
   Understanding your org's current level of risk and acceptable risk
4. **Building knowledge**
   on PQC and its impact
5. **Best practices**
   Developing TLS best practices internal to your org

In terms of their specific activities, "monitoring" was (not surprisingly) the top tactic currently employed by IT. Understanding their organization's level of crypto-agility came next. This reflects the understanding that when the time comes to make a switch to PQC certificates, enterprises need to be ready to make the switch quickly and efficiently.

Rounding out the top five were the objectives of understanding the organization's current level of risk, building knowledge about PQC and developing TLS best practices.

Characterizing the Quantum Computing fight

IT is clear about the cryptographic risks they face from quantum computing. First, IT worries that the cost of fighting future quantum computing threats/attacks will spiral out of control. Second, they're concerned that data safely encrypted by today's standards will become easy to decrypt in a quantum future. That means data pilfered today may be safe for now, but could become vulnerable once quantum computers arrive.

There is a similar fear about IoT devices. Engineered using today's best cryptography means these devices are safe from today's attacks, but will be vulnerable to future quantum attacks. For long-lived products such as cars or ATMs that becomes a big issue.

Thus, IT has committed to fight the quantum battle. Why? The expected benefits of winning this battle include improving the company's security, ensuring communications are protected from being decrypted in the future and, finally, improving crypto-agility.

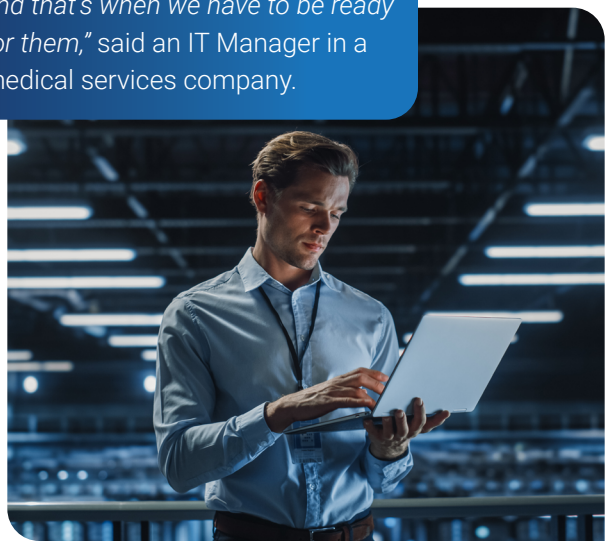
This final benefit—crypt-agility—is a tactical admission that the world of cryptography will change quickly in the future and that enterprises need to be able to swap old algorithms for new quickly without bringing down their networks.

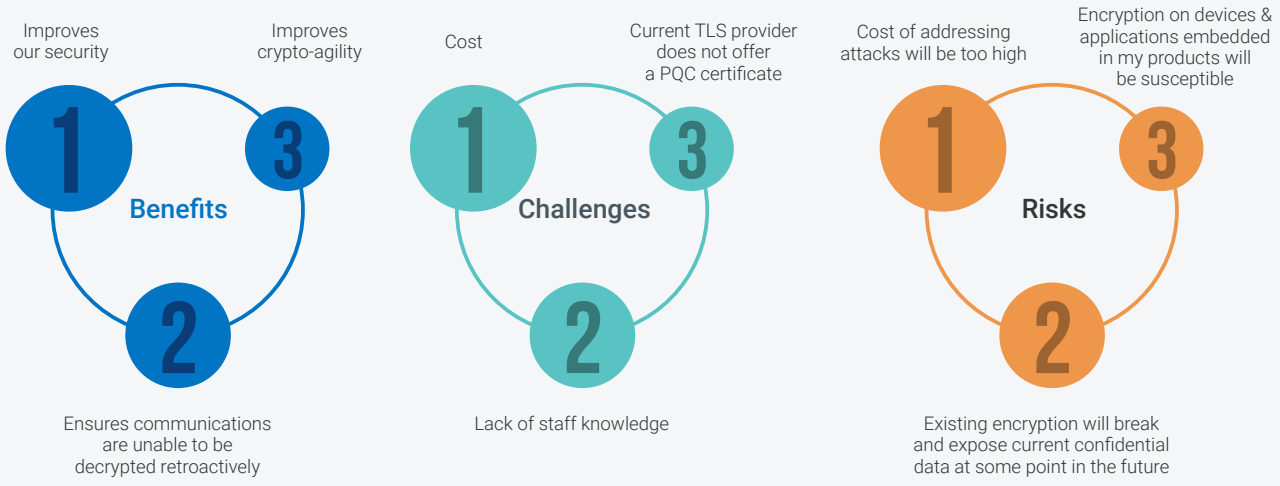
While these benefits are worth fighting for, there are challenges that IT recognizes in the quantum battle.

The biggest challenge—according to respondents—is cost. This is exacerbated by a general lack of staff knowledge about quantum attacks and how to defend against it. Finally, a common fear mentioned was that the current TLS vendor may not offer a sufficient PQC certificate in time.

On balance, IT is realistic about the challenges they face. In fact, nearly two of five say it will be somewhat to extremely difficult to upgrade encryption to protect against quantum computing attacks.

"In the future, it's going to happen and that's when we have to be ready for them," said an IT Manager in a medical services company.





DigiCert recommendations

Quantum computing is one of the three key technologies that will shape a company's future.

Yet quantum's promise is tempered by the risk it poses to cryptography. DigiCert, the world leader in cryptography for the web, offers the following recommendations for companies ready to start planning their strategies for securing their organizations for the quantum future.

Risk
Know your risk and establish a quantum crypto maturity model

Ability
Understand the importance of crypto-agility in your organization and establish it as a core practice

Best Practices
Work with leading vendors to establish digital certificate best practices and ensure they are tracking PQC industry progress to help you stay ahead of the curve, including with their products and solutions. Change rarely happens quickly, so it's better not to wait, but to address your crypto-agility now.

About DigiCert, Inc.

DigiCert is the world's leading provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs its award-winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world. For more information, visit digicert.com or follow @digicert