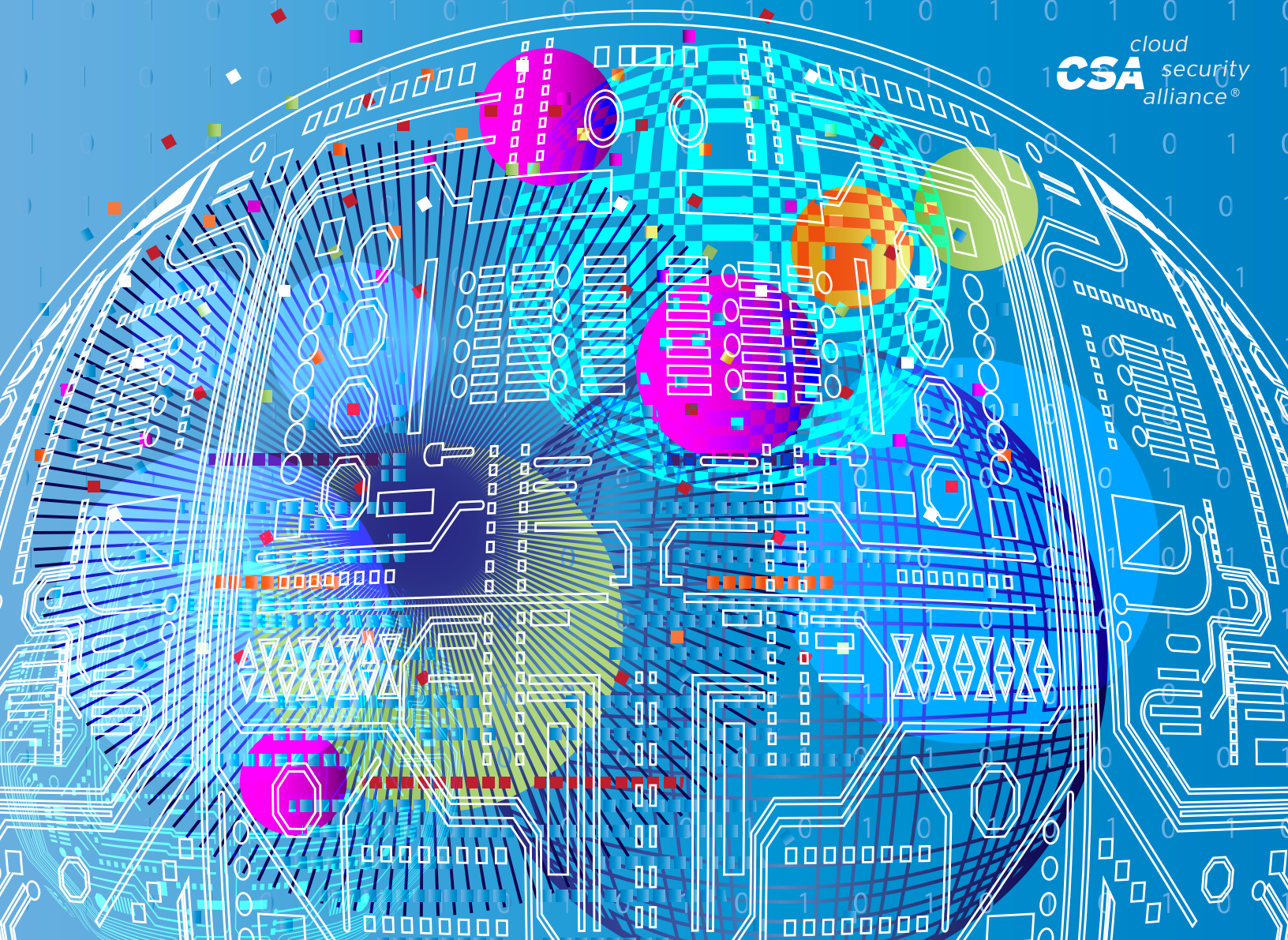
Quantum-Safe Security Awareness Survey

Presented by the QSS Security Working Group



cloud security alliance®

ABOUT CSA

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at www.cloudsecurityalliance.org and follow us on Twitter @cloudsa.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Quantum Safe Security Working Group (QSS) of the Cloud Security Alliance (CSA)[1] recently conducted a survey of CSA members to ascertain overall awareness of quantum security risk within the cloud computing community . The survey's findings show that most cloud computing representatives are aware of the risks and would like to learn more, but many of these people are not willing or able to act upon that goal at this time. The inability to act is due to a perception that few solutions exist, in addition to a dearth of resources.

The QSS recommends that companies should begin assessing their own quantum risk. Given how rapidly the risks are progressing, QSS also recommends immediate implementation of quantum-safe solutions in order to future-proof today's data from tomorrow's attacks.

1 CSA is a non-profit organization with global membership. CSA promotes the use of best practices for providing security assurance within cloud computing, and educates members about how cloud computing cansecure all other forms of computing.

RATIONALE FOR CONDUCTING A QUANTUM-SAFE SECURITY AWARENESS SURVEY

Quantum computing threatens the security of public key cryptography, which underlies our global digital communications infrastructure. While many significant challenges must be overcome in order to realize a cryptographically useful quantum computer, the quantum computing community now believes this goal could be reached within the next 10 to 15 years. Therefore, cloud computing professionals need more information about the threats, including, of course, how to counteract them effectively.

In order to fill the information gap, the QSS recently conducted a survey of CSA members about their overall awareness of quantum security risks and approaches to tackle these risks.

The aim of this document is to share the most significant findings from the survey in order to identify areas of potential concern and action. The complete list of survey questions and responses can be obtained from the QSS upon request.[2] We recommend that interested readers also read the QSS document entitled "Quantum Safe Security," which describes the threats from quantum computing and outlines approaches to tackle them.

The participants in this survey were all members of CSA, with an overwhelming majority (more than 90 percent) of professionals working in Information Technology or Information Security. This means that, overall, they are both better informed about security issues and better versed in security solutions than the general population. Ninetry-three percent of the companies they represent use encryption to some extent to protect their data, as compared to forty-one percent of typical enterprises in 2015[3]. Therefore, we expect these companies to be indicative of organizations which highly value security and the implementation of best practices. Due to the low response rate, this survey does not present a statistically significant sample. However, we believe it does provide a valuable snap-shot of the perception of quantum-safe issues in the industry.

2 The data will be provided free of charge. Proper acknowledgement of the source will be required if information is distributed. Contact the CSA Research Team, research@cloudsecurityalliance.org to obtain a copy.
3 2016 Ponemon Thales Encryption Application Trends

A first set of survey questions investigated overall awareness of quantum computing risk.

As shown on the left side of Figure 1, sixty percent of respondents were “very aware” or “somewhat aware” of quantum computer technology and of the impact that quantum computers may have on data security. Only 14 percent were “not aware at all.” In addition, a majority of respondents (nearly 70 percent) also understand that their data is at risk. Confidence in current security approaches against quantum computer risks is generally low: 30 percent of respondents were “very confident” or “somewhat confident” that their current security approaches do keep their data safe, as shown on the right side of Figure 1.

The conclusion is that most respondents are aware of the issue, understand that their data will be at risk, and do not trust their current solutions.

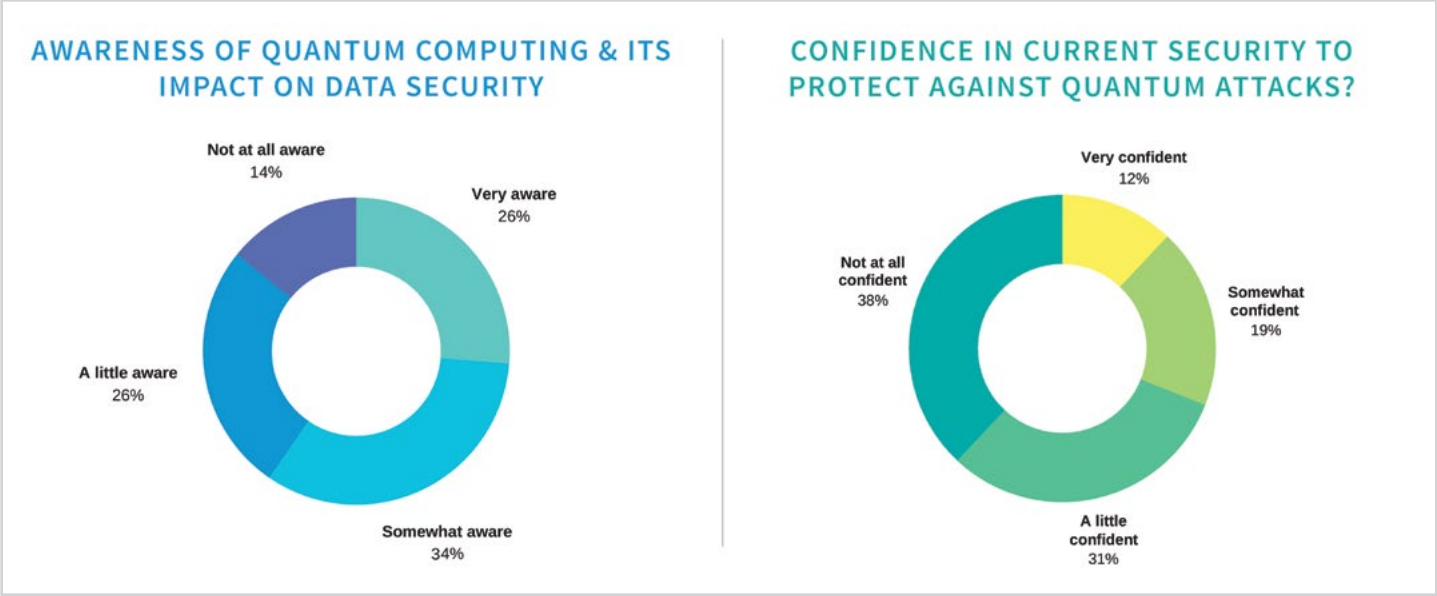


Figure 1: Impact of the Quantum Computer on security (left); and confidence of current security against quantum attacks (right)

Understanding the threat is a first step. What we now need is to consider possible solutions, known as quantum-safe technologies.

Here, the results are a bit more mixed. Nearly half the respondents (47 percent) neither agree nor disagree that there are quantum–safe technologies in the market that can help protect against quantum-based cyber-attacks.

Twenty-three percent "disagree" or "strongly disagree," while only 30 percent agree or strongly agree. **Clearly, most respondents do not believe there is an existing solution to the quantum computing threat.**

This is an important result: it is our responsibility as professionals to educate the computing community about quantum-safe solutions. In fact, this is clearly one of the goals of the QSS-WG

Actually, commercially available solutions to this problem exist today. They include quantum random number generators and quantum key distribution technologies, both of which can help reduce the risk. In addition, there are many additional activities ongoing in the quantum-safe space which will complement these technologies and enable stronger quantum safe protection in the next few years. The organizations responsible for establishing computing safety standards in both Europe and the United States have shown interest in implementing quantum-safe cryptography. For example, ETSI, ISO and NIST are actively investigating quantum safe solutions.

In 2015, ETSI published a whitepaper[4] urging stakeholders to begin investigating and ultimately adopting quantum resistant cryptography. In August 2015, NSA released a notice[5] that they would be revamping Suite B cryptography to include quantum resistant solutions. NIST's call for proposals for quantum-resistant, public-key cryptographic algorithms closed on November 30, 2017, and is now being followed by an analysis and selection phase.

Although many respondents do not believe a solution currently exists to counteract quantum threats effectively, most are familiar with some aspects of quantum-safe technologies This is shown in Figure 2, to the right. Only 20 percent of respondents had no knowledge of such technologies. The most well-known answers to quantum threats are the use of longer symmetric keys and hash functions. Approximately half of respondents were aware of each of these security technologies. This is in agreement with the fact that symmetric key crypto is known to withstand the threat, at the cost of doubling the key sizes. So, the perception of the threat of the quantum computer on symmetric cryptography seems to be adequate. Quantum random number generators, which generate high quality keys, is second, close to both Quantum Key Distribution and Quantum safe Algorithms, all reaching approximately 30 percent awareness, which is an inadequate number. Again, there is a need for better education of our colleagues.

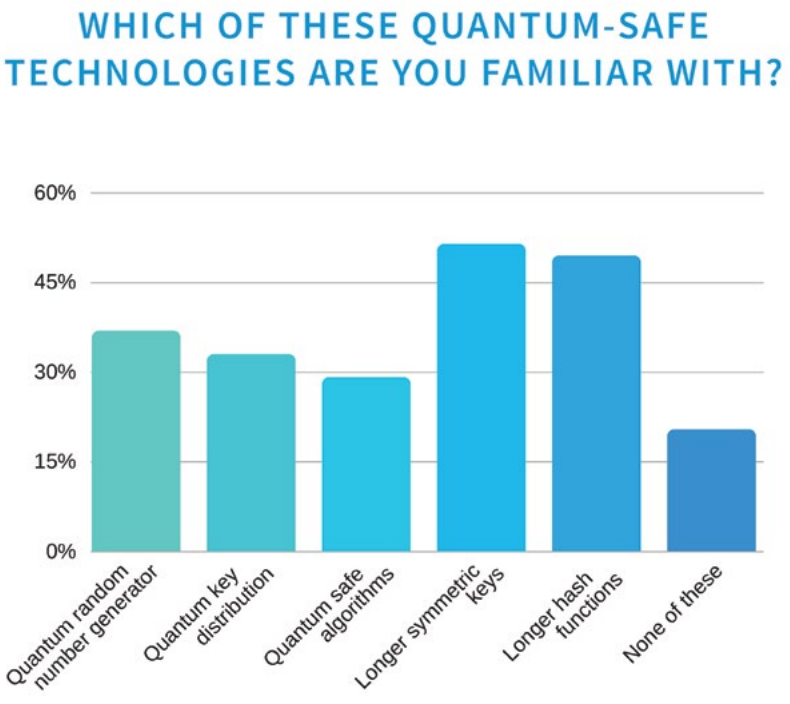


Figure 2: Familiarity with quantum-safe technologies

4 https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
5 https://www.nsa.gov/ia/programs/suiteb_cryptography/

Taking into account the high level of awareness discussed above, it is rather surprising to discover that most companies are not taking any action to tackle the threat. Indeed, only 40 percent of surveyed companies (see Figure 3, below) are working to future-proof their data against the quantum computer threat.

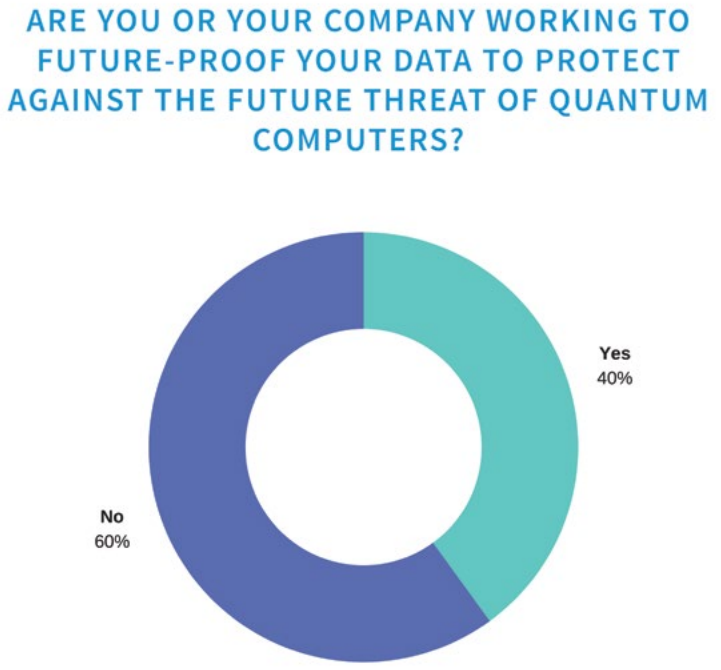


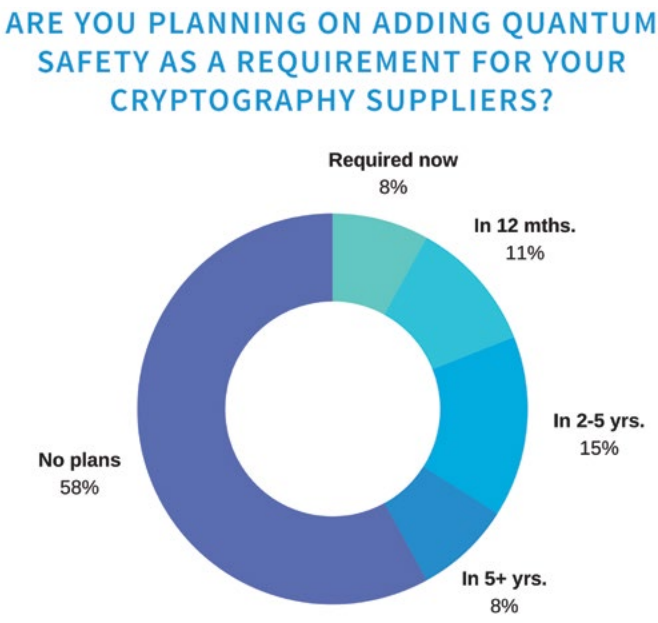
Figure 3: Action taken to protect data

There is clearly a disconnect between awareness of quantum security issues, in-depth understanding of the potential threats, and willingness to act upon this knowledge effectively.

The question was then extended to more details, as shown in Figure 4, below right.

Sixty percent of respondents are not engaged in protecting their data from the future threat of quantum computers. The most alarming piece of the entire survey is that many of those companies that say they are not currently acting on this threat, also say they do not have plans to do so for at least three years, if at all, and are not planning to include quantum-safe cryptography as a requirement for their technology suppliers. This makes their data vulnerable to harvesting attacks, in which data is downloaded and then stored for later decryption by quantum computers.

Quantum computers will be able to break all public key systems, which underlie essentially 100 percent of the key exchange and digital signature systems in use today. A quantum computer will render all these systems vulnerable, and is predicted to exist



within the next 10 to 15 years.[6] A transition from current cryptography to quantum-resistant cryptography, even in the most optimistic of estimates, would take a decade or more.[7]

So why are so many companies not acting now, as the reality of quantum computers draws near? Our survey reveals two main reasons, shown here:

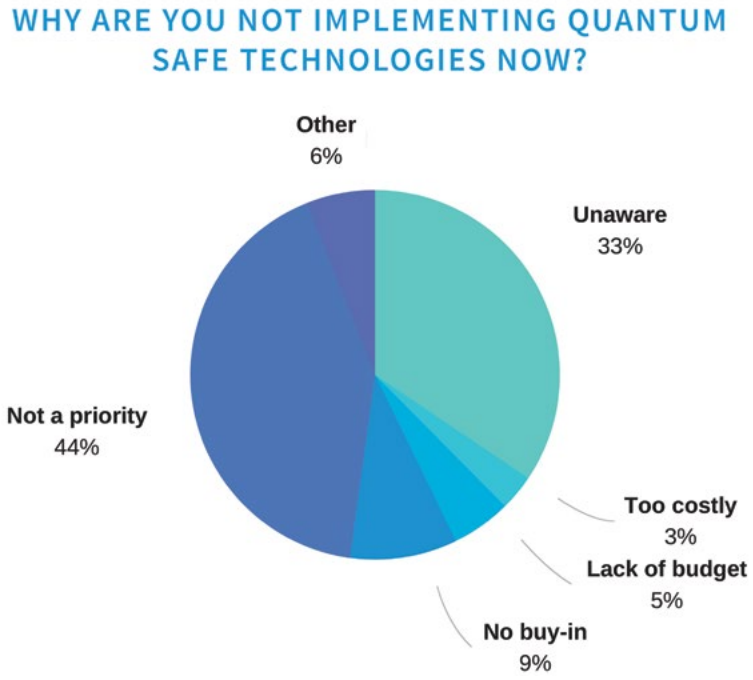


Figure 5: Reasons behind poor implementation of Quantum-safe solutions

First, forty-four percent state that securing these risks is not a priority. One can imagine that other issues, seemingly more urgent are taking the resources of many IT and Security teams, preventing them from addressing this threat. For companies managing personal or financial data, or with other data that has a security life of more than a few years, this choice of priorities may end up hurting them and their clients in the future, as they will be those most vulnerable to the harvesting attacks described above. This underlines the important role of information and education needed to ensure that companies appropriately prioritize resources.

Second, thirty-three percent of respondents are unaware that solutions to these threats exist, rather in line with the results of Figure 2. This is underscored by the result that the most frequent response to the statement "Quantum solutions are currently available" is that they neither agree nor disagree. Clearly communication is needed to allow people to give a more informed response!

Other survey responses indicate a lack of buy-in from key decision makers (9 percent), lack of budget (4.5 percent) and believing solutions are too cost-prohibitive (3 percent).

6 http://arxiv.org/abs/1510.03859
7 One need only look at the past 20 years, with the call for increased RSA key size from 1024 to 2048-bit and the call for the transition from RSA to elliptic curve based cryptography, neither of which required the level of hardware and software change that the upgrade to quantum resistant cryptography requires to appreciate just how optimistic this "10 year" transition period is.

HIGH INTEREST IN LEARNING MORE ABOUT QUANTUM-SAFE TECHNOLOGIES

To end on a positive note, while most companies are not yet taking action, interest level is high, hopefully a good sign for the work ahead to help inform and prepare our society for the next big security threat. This is shown in Figure 6, below.

Figure 6: Interest in quantum-safe technologies

The QSS-WG, and the CSA as a whole, clearly have to continue and expand their efforts towards reaching out to companies and explaining the issues. There is a real appetite for better education. We have to fulfill it.

CONCLUSION

This survey reveals the long path to convincing companies who maintain client data of how important it is to include solutions to the threat of quantum computing in their overall security strategies. While aware of the issue and familiar with some aspects of quantum-safe technologies, most companies are not taking action yet. On the good side, many express interest and l want to know more. Education about this important topic has to be continued.

The complete results of the survey are available from the CSA upon request. They can be freely used and cited, with proper acknowledgement.