Report Response

Researchers have identified that quantum computers could enhance the processing power we have today through classical and supercomputers. Their existence, however, could also break all public-key cryptographic algorithms we use today for securing electronic communications (Aumasson, 2018). Quantum computing can be a threat in a little more than a decade or even sooner (Giles, 2019a) if stable and full processing power versions of these computers are built. Hence, our organization needs to consider NIST’s recommendation to switch to the new algorithms (Hanacek/NIST, 2016) expected to be standardized in 2022 (Giles, 2019b) to protect ourselves from current and future attacks (Hanacek/NIST, 2016). We should also require vendor solutions to include quantum-resistant cryptography (QRC) algorithms to keep our data safe before the existing algorithms are compromised. However, these new algorithms can be a threat too if they get implemented without proper understanding (Aumasson, 2018) or if attackers find ways to exploit them, whether deployed before or after quantum computers. Therefore, we should also develop third party management (TPM) risk policies to address and mitigate the risks these technologies can pose and protect our data. After all, we know that these algorithms are going to be embedded in our many different systems (Giles, 2019b).

References

Aumasson, Jean-Philippe. (2018). *Serious Cryptography*. San Francisco, CA: No starch press.

Giles, Martin. (2019a). MIT Technology Review Explainer: What is a quantum computer? Retrieved from https://www.technologyreview.com/s/612844/what-is-quantum-computing/

Giles, Martin. (2019b). MIT Technology Review Explainer: What is post quantum cryptography? Retrieved from https://www.technologyreview.com/s/612844/what-is-quantum-computing/

Hanacek/NIST. (2016). NIST Kicks Off Effort to Defend Encrypted Data from Quantum. Retrieved from https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat