kloke™
ai-driven security

Which Data Security Story Ending Do *You* Prefer?

From 'Horror' to 'Happy' — and Many More In Between

by Doug Peckover | April 2019

Here's how this story starts: According to Microsoft, the new quantum computers will solve problems in 100 seconds that would take a classical computer one *billion years*. That's not a typo! This new computing power puts today's encryption-based data security at risk because its premise is based on math being 'difficult.'

The big question is when will this 'quantum risk' begin?

If you prefer short stories, you'll like research suggesting that quantum computers may not break encryption for decades. So, sit back, relax and do nothing.

If you prefer a story ending with a bit more drama, your encryption will be broken within a few years because 99 percent of online encryption is vulnerable to quantum computers, according to Mark Jackson, scientific lead for Cambridge Quantum Computing. With this ending, start planning now for a massive code review. The cost for such an undertaking is unknown, but the last major code review was for Y2K, which cost an estimated $400 billion worldwide and took years to complete.

If you like scary endings, IBM is calling the quantum computer threat 'imminent,' suggesting it will affect nearly all encrypted data on personal devices, communications, private databases, smart vehicles and government databases. That, indeed, is a *very* scary ending.

If horror stories are your thing, you'll love the one from Rep. Will Hurd, Chairman of the House Oversight and Reform IT subcommittee. He says "whoever gets to true quantum computing first will be able to negate all the encryption that we've ever done to date. That is why China [and] Russia are sucking up ciphertext." Translation: the quantum threat *already exists*.

If you're into nightmares, one comes from a mathematician at the National Institute of Standards and Technology (NIST — the standards body working on quantum-resistant cryptography) who said, "It will take 10 to 20 years to get new algorithms selected, standardized and implemented out into the field." A related story goes on to state that NIST "must evaluate each [solution] against both classical and quantum attacks to ensure that the problems are still difficult to solve, with the hopes of drafting updated standards by 2022 to 2023." Three words make this story a nightmare — 'difficult,' 'hope,' and '2022.'

There's one more story ending to consider — one with a happy ending. Unlike the nightmare, its three words are 'simple, 'proven,' and 'now,' because a remarkable data security solution already exists — 'tokenization' — proven by financial institutions (and protecting credit card transactions) for more than a decade. A U.S. firm has seven patents that upgrade tokenization security, making all data quantum-safe — from IoT devices and blockchain ledgers, clear up to legacy databases.

However, the most remarkable benefit of such an enhanced tokenization security solution is that, unlike potential encryption options still years out on the horizon, upgrading existing systems is seamless, requires little or no programming changes, won't cost the industry billions or take years to deploy.

For firms and government agencies ready to take advantage of this simple — and immediately available — quantum-safe security solution, their story has a happy ending.

About the author: Doug Peckover is Co-Founder and Chief Scientist at Kloke — a developer of AI-driven data security solutions. He holds numerous data security and technology patents.