SEAGATE | GOVERNMENT SOLUTIONS

: Designing Storage Architectures for Digital Collections

September 17-18, 2018

LIBRARY LIBRARY OF CONGRESS

Quantum is coming

THE IMPACT WILL BE DRAMATIC

- Data volume impact
- Data usage impact
- Security impact
- Archive Impact

What about?

BUT HENRY QUANTUM WILL NOT REPLACE VON NEUMANN COMPUTERS

- "Quantum computers will never be able to run the if/then/else type of logic that we're familiar with our traditional Von Neumann architecture computers, [where they are] sequentially going from step to step," said Andy Stanford Clark, IBM CTO for UK and Ireland.
- Quantum computers excel at optimization problems "Quantum computers are really good at solving those problems where you've got an exponential number of permutations to try out," said Stanford Clark.
  - "If, for example, you're optimizing the lengths of aircraft routes, or optimizing the layout of spare parts for a rail network, something where there's 2n possibilities and you've got to try each out in order to find the optimal solution.
  - (https://www.techrepublic.com/article/quantum-computing-seven-truths-you-need-to-know/)
    - July 24, 2018

The Threat to Encryption real

WE NEED A PLAN

- Quantum computers will be able to instantly break the encryption of sensitive data protected by today's strongest security, warns the head of IBM Research.
  - This could happen in a little more than five years because of advances in quantum computer technologies. "Anyone that wants to make sure that their data is protected for longer than 10 years should move to alternate forms of encryption now. Quantum computers can solve some types of problems near-instantaneously compared with billions of years of processing using conventional computers" said Arvind Krishna, director of IBM Research
- The time is now for archives

Quantum Players and customers

BIG NAMES BIG BETS

- Google
- Microsoft
- Intel
- IBM
- China
- D-Wave Systems
- Customers
  - Los Alamos Labs
  - Oak Ridge National Lab
  - Lockheed Martin
  - NASA Ames
- **There is too much money and too many big names for Quantum not to happen**

What NIST is saying is at risk

HTTPS://CSRC.NIST.GOV/PUBLICATIONS/DETAIL/NISTIR/8105/FINAL

Cryptographic Algorithm	**Type**	**Purpose**	**Impact from large-scale quantum computer**
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	---------------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Seagate

The End, Chicken Little presentation completed

Back to your regularly scheduled presentations with happier thoughts from others.