ADDRESSING THE QUANTUM COMPUTING THREAT TO CRYPTOGRAPHY

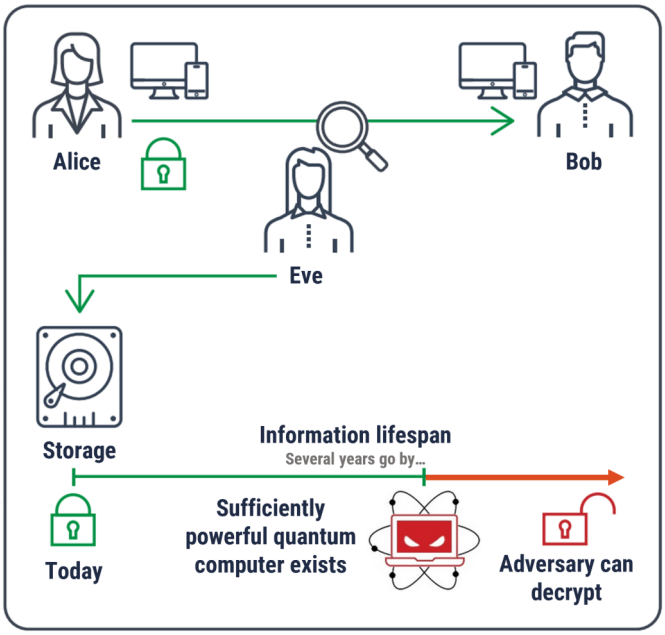
MAY 2020 ITSE.00.017

Cryptography is an effective way to protect the confidentiality and integrity of information and to protect IT systems from cyber threat actors. Quantum computing threatens to break much of the cryptography we currently use. Quantum computers will use quantum physics to efficiently process information and solve problems that are impractical to solve using current computing capabilities. Quantum computers that are available now are not sufficiently powerful enough to break cryptography, but the technology is advancing quickly and could be available by the 2030s. However, threat actors can steal encrypted information now and hold on to it until a sufficiently powerful quantum computer is available to decrypt, read, or access the information, even well after the information was created.

INFORMATION LIFESPAN

Information lifespan refers to the timeframe for which information held by your organization requires protection (e.g. to protect privacy or intellectual property).

Threat actors can store encrypted information and decrypt it in the future when a sufficiently powerful quantum computer exists. Therefore, information with a medium or long lifespan (i.e. it will still require protection in 10 or more years) could be at risk of being decrypted by threat actors.



Eve can capture and store information right now that has a medium or long lifespan to decrypt when a sufficiently powerful quantum computer exists.

Need help or have questions? Want to find out more about cyber security? Visit the Cyber Centre website at **cyber.gc.ca**

FUTURE TECHNOLOGY

Future quantum technology and quantum key distribution (QKD) may be used to protect sensitive information. Research on the security and the scalability of QKD is progressing, and the development of QKD is still maturing. QKD is not a replacement for current applications of cryptography, but it could be a way of securely communicating in the future.

The Cyber Centre is working with NIST[1] and other partners to develop the next generation of quantum-resistant cryptography for traditional computers (e.g. to replace current cryptographic applications). Integrating these new components will require software and hardware updates to existing IT systems, which may require significant investments.

MANAGING THE RISK

We recommend the following three steps to manage the risks associated with quantum computing advancements:

1. Evaluate the sensitivity of your organization's information and determine its lifespan to identify information that may be at risk (e.g. a part of on-going risk assessment processes).
2. Review your IT lifecycle management plan and budget for potentially significant software and hardware updates.
3. Educate your workforce on the quantum threat.

Contact the Cyber Centre (contact@cyber.gc.ca or 1-888-CYBER-88) for more information and guidance.

REFERENCES

The Cyber Centre and NIST[1]: *Post-Quantum Cryptography.*

EXECUTIVE SERIES