MAY 24
Jenna McNamee

Risk mitigation for quantum computing starts with a strong encryption plan

Article

What we're watching: Though quantum computing may be years away from being fully operational, **financial institutions (FIs) must begin** preparing for its risks now. Here's what

banks can do today to make sure their data is safe in the future, according to a report by the Financial Services Information Sharing and Analysis Center (FS-ISAC).

The long game: Experts at FS-ISAC are warning banks that even data that's currently encryption-protected is at risk.

- Any time encrypted data leaves its data center, it can be stolen. Though hackers and bad actors may not have the tools to decrypt the data, they still collect and store the data in a scheme called "harvest now, decrypt later."
- The hackers hold on to the data with the intent of decrypting it once they develop or gain access to quantum computing technologies that can access it.

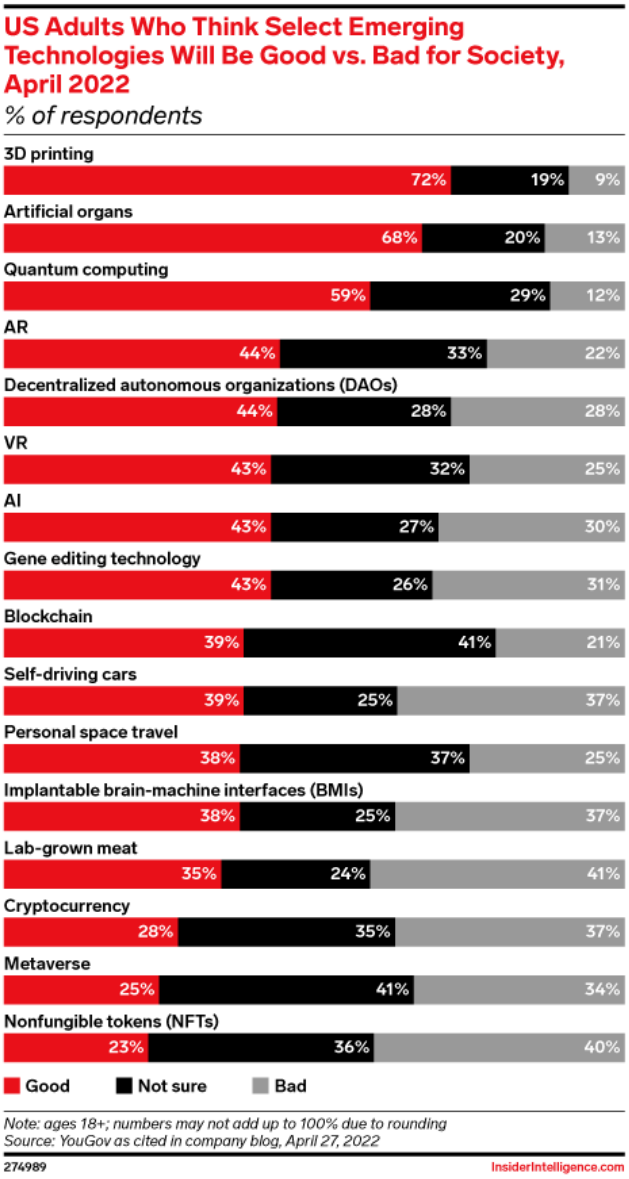
Encryption best practices: There are a few things FIs can do to prepare for future quantum computing risks.

- **Document all instances where encryption is used.** This is the first and easiest step. A catalog of encrypted data serves as a reference that easily identifies data that could potentially be at risk.
- **Use multi-layer security.** Pairing classical encryption methods—algorithms like RSA and ECDSA—with other protections like authentication technology and data fragmentation won't protect the data from quantum computing. But it will require hackers to break through several layers of security.
- **Apply the National Institute of Standards and Technology (NIST)-recommended Crystals-Kyber algorithm.** This algorithm, which offers an additional layer of protection, is believed to be resistant to classical and quantum computing decryption—so far, no computer has been able to break it. Though this algorithm isn't necessary at this time, it could add a strong level of defense in the future.

The big takeaway: New technologies are revolutionizing the way banking is done. But they're also pressuring banks to ensure their risk controls are in tip-top condition.

- Building out flexible encryption capabilities and keeping an inventory of all areas where encryption is used can position FIs to stay ahead of quantum computing risks.
- But risk mitigation shouldn't just apply to quantum computing. Risks accompany all tech innovation, from artificial intelligence to the metaverse. FIs that only focus on the positive

side of innovation may find themselves unprepared and potentially out of business in the face of risk.



*This article originally appeared in Insider Intelligence's **Banking Innovation Briefing**—a daily recap of top stories reshaping the banking industry. Subscribe to have more hard-hitting takeaways delivered to your inbox daily.*

- *Are you a client? Click here to subscribe.*
- *Want to learn more about how you can benefit from our expert analysis? Click here.*