The Cybersecurity Readiness Podcast Series

Episode Title	Future-Proofing Your Data: Preparing for the Post-Quantum Era
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	David Close, Chief Solutions Architect, Futureex
Summary Pitch	Dr. Dave Chatterjee and David Close discuss the implications of post-quantum cryptography (PQC) on cybersecurity readiness. David, a Chief Solutions Architect at Futurex, explains the evolution of cryptographic methods to counter quantum computing threats. He highlights the importance of NIST's role in standardizing quantum-resistant algorithms like Kyber and Dilithium. David shares practical examples, such as Google and Cloudflare's hybrid TLS implementation and a financial institution's use of PQC for data storage. They emphasize the need for organizations to develop roadmaps, inventory cryptographic assets, and ensure vendor readiness. Dr. Chatterjee stresses the importance of a proactive, holistic approach to cybersecurity governance.
Action Items and Discussion Highlights	▪ Inventory all cryptographic assets across the organization. ▪ Assess and prioritize high-risk data that needs to be protected against quantum attacks. ▪ Evaluate the organization's crypto agility and ability to support hybrid encryption schemes. ▪ Test PQC-enabled TLS and other PQC implementations in a pilot environment.

	▪ Develop a rollout plan for transitioning to PQC algorithms in alignment with NIST recommendations. ▪ Provide training and awareness on PQC to engineering and security teams.
Time Stamps	00.00 – Introduction 01:56 – Guest's Professional Journey Highlights 04:12 – Overview of Quantum Computing 08:37 – "Harvest Now and Decrypt Later" Reality 11:11 -- Testing Post-Quantum-Cryptography 14:09 – Financial Services Use Case 16:49 – Roadmap to Quantum-Safe Readiness 24:05 – Three Pillars of Proactive Cybersecurity 28:06 – Challenges and Best Practices 32:22 – Closing Thoughts
Memorable David Close Quotes/Statements	"Quantum computing is a major threat in today's cryptography." "So right now, companies like IBM and Google, have built early-stage quantum computers with 10s to hundreds of qubits. They're still noisy and limited but improving very quickly." "Quantum bits or qubits are extremely sensitive; they can be thrown off by heat, vibrations, even stray electromagnetic fields. And that's what I mean when I say noise. It causes errors in calculations, which is a huge challenge, because quantum algorithms, like Shor's algorithm that I mentioned, requires long, precise operations and until we have error corrected qubits, today's machines can't run those powerful algorithms reliably."

	“Traditionally, organizations rely on encryption protocols like TLS, but with quantum computing on the horizon, it's not enough.” “Quantum computing is a digital storm that's on the horizon.” “Quantum computing, really is the next wave of innovation for cryptography, but it also brings real risks.” "If we wait till quantum computers are fully here, it will be too late. So that's why you need to build crypto agile systems now and deploy quantum safe algorithms now and make sure your vendors, including your HSM vendors, are ready to protect your most valuable keys. But the good news is we have the materials NIST gave us, the roadmap. PQC is here, and HSMs are ready. So now it's time to build those levees." “Most engineers and security architects may not be familiar with PQC, and that creates friction, so invest in training programs. Some of them may be vendor LED or led by outside organizations, to make PQC part of your secure coding guidelines.”