The Cybersecurity Readiness Podcast Series

Episode Title	Quantum Computing and Cybersecurity – Examining Trends and Implications
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Duncan Jones, Head of Cybersecurity, at Quantinuum.
Summary Pitch	The fast-evolving quantum computing phenomenon represents a paradigm shift in how computers process data. Due to its ability to process vast amounts of data and solve complex problems at an unprecedented speed, quantum computing holds great promise for new material discovery through the simulation of physical systems, portfolio optimization in finance, and more. It also poses a significant threat to cybersecurity, requiring a change in how we encrypt our data. Even though quantum computers don't technically have the power to break most of the current forms of encryption yet, we need to stay ahead of the threat and come up with quantum-proof solutions now. If we wait until those powerful quantum computers start breaking our encryption, it will be too late. I had the pleasure of discussing the quantum computing phenomenon and its cybersecurity implications with Duncan Jones, Head of Cybersecurity, at Quantinuum. We discussed the potential threats and opportunities of quantum computing for cybersecurity, as well as its potential to revolutionize various industries. We recognized the need for new algorithms resistant to quantum computing, staying ahead of technological innovations, investing in cybersecurity measures, and

	prioritizing the migration of sensitive data to quantum-resistant algorithms. **Action Items** 1. Assess organizational risk exposure from quantum computing threats like "store now decrypt later" attacks. 2. Prioritize migration of sensitive long-term data to quantum-safe encryption. 3. Speak to vendors about their roadmaps for quantum-safe migration. 4. Explore available quantum random number generators and other quantum cybersecurity technologies through pilot programs and starter kits. 5. Choose credible service providers who are partnering with reputed organizations and prove their claims. 6. Raise awareness of quantum computing implications among leadership and get buy-in for piloting relevant quantum cybersecurity technologies.
Time Stamps	00:02 -- Introduction 01:59 -- Guest's Professional Highlights 06:19 -- Overview of Quantum Computing 08:19 -- Commercially Leveraging Quantum Computing 10:51 -- Evolution of Quantum Computing and Cyber Attacks 12:55 -- Recommendations on Leveraging Quantum Computing Benefits and Securing Data from Quantum Computing Enabled Cyber Attacks 17:49 -- Roadmap for Proactive Safeguards

	23:34 -- Can quantum computing enabled encryption ensure that even if a human is a victim of a phishing attack, it will be hard to get into systems? Is that a fair aspiration? 26:38 -- What recommendations would you make for organizations who are trying to explore and adopt quantum computing? 29:19 -- Cybersecurity Challenges and Hurdles 32:52 -- Challenges of Quantum-Safe Migration 34:09 -- Cryptographic debt 37:32 -- Final Thoughts
Memorable Duncan Jones Quotes/Statements	"I think of my career as a series of very fortunate accidents, rather than some very carefully planned out thing." "Quantum computing as a different form of computation, as opposed to necessarily always a better form of computation." "Leading companies are now starting to engage with quantum computing because they know they have to build the skill sets, they have to develop the intellectual property that will begin to deliver value in the not too distant future." "Quantum computers are becoming more and more powerful every year." "We'll actually see Quantum as a as a big benefit for cybersecurity, but we've got some headaches to get through first." "Every cryptographic system is going to need to change to move to these new algorithms that are believed to be quantum resistant."

	"Store-now-decrypt-later approach represents the idea that you have some persistent threat actors, people who really, really genuinely want to get some of the data that you have, and they're willing to patiently wait more than 10 years, potentially, to crack into something that they've stolen from you." "I think it's all about focusing on a defense in depth approach. And making sure every layer in your system is as secure as possible. And where quantum can actually provide some really strong benefits is in those lower layers." "It basically boils down to generating unpredictable random data." "With quantum technology, you can take some risks off the table, but just not all risks." "What I'm discovering is that organizations don't always know what they have." "Quantum is a really good thing for cybersecurity, it's a wonderful excuse to make our systems better. It's a wonderful excuse to get rid of the cryptographic debt that has been piling up for a few years. And then by embracing the technology itself and weaving it into our everyday systems, we're actually going to make them stronger than before. So I would say quantum is a gift for cybersecurity."