ProteQC® Co-Founder Darren Bender Presents 'Post-Quantum Negligence' in PQShield Podcast Interview

New interview explores how delaying post-quantum cryptography could expose organisations to future legal liability

LONDON, UNITED KINGDOM, March 12, 2026 /EINPresswire.com/ -- ProteQC®, a cryptographic resilience advisory firm, highlights a recent podcast interview with PQShield, the market leader in post-quantum cryptography (PQC), featuring co-founder and Chief Legal Officer Darren Bender, who introduced the emerging concept of "Post-Quantum Negligence." The episode builds on ProteQC's mission to help organisations achieve cryptographic resilience, ensuring their systems can adapt quickly as standards evolve.

Post-Quantum Negligence, a term coined by U.S. litigation attorney Darren Bender, describes what could become a new category of legal exposure as the risks of quantum computing become widely understood. In the interview, "Post-Quantum Negligence: When Inaction Becomes Legal Exposure," on the cybersecurity podcast Shielded: The Last Line of Cyber Defense, Bender introduces the concept and explains how failing to prepare for quantum threats today could create future legal liability for organisations that delay cryptographic migration. The episode has already exceeded 96,000 YouTube views—a notable milestone for a subject at the intersection of quantum physics, cybersecurity, and law.

Johannes Lintzen, Global Director of Business Development at PQShield and host of the Shielded podcast, said: "This conversation reflects exactly why we started the Shielded podcast, to have honest, practical discussions about what the quantum shift really means for the people responsible for protecting systems today. At PQShield, we work closely with organisations that are actively transitioning to post-quantum cryptography, and we see firsthand that this is no longer a theoretical issue. It is easy to frame quantum computing as a distant milestone, but for security teams and boards, the question of how to reduce exposure now is already on the table. Darren's perspective brings that reality into sharp focus. As understanding of quantum risk grows, so will expectations. These conversations matter because they help turn a complex technical challenge into a clear, responsible plan of action."

While the industry frames post-quantum cryptography as a future technical upgrade, Bender argues that courts may view the issue differently. That is, through the established legal principles of duty of care, foreseeability, and negligence. "Quantum risk is often treated as a distant

engineering challenge," said Bender. "But once a risk becomes widely known and reasonably foreseeable, organisations may have a legal duty to address it. The question courts will ask in the future is simple: what did you know, and what did you do about it?"

In the interview, Bender outlines three emerging risks organisations should consider as quantum computing advances:
- Harvest Now, Decrypt Later attacks: Adversaries may collect encrypted data today with the expectation it can be decrypted once large-scale quantum computers emerge. Because sensitive information—such as financial, healthcare, and intellectual property data—can remain valuable for decades, organisations that delay post-quantum planning could face future exposure.

- Performative quantum readiness: Bender cautions against organisations claiming quantum readiness without meaningful cryptographic migration or governance behind those claims. Courts may not expect perfection, but they will expect evidence that organisations took reasonable steps to understand and manage the risk.

- Emerging negligence exposure: As quantum risk becomes legally foreseeable, organisations that cannot demonstrate reasonable preparedness may face liability under established tort principles—including the Learned Hand test.

ProteQC was founded to help financial institutions prepare for the transition to post-quantum cryptography and reduce emerging governance and legal risks associated with quantum computing. "Preparing for the quantum era isn't just about cryptography," Bender added. "It's about governance, documentation, and ensuring organisations can demonstrate responsible decision-making when new technological risks emerge."
To learn more about the concept of post-quantum negligence and how organisations should prepare for the legal and security implications of the quantum era, listen to the full podcast on major podcast platforms or watch the video version on YouTube:
https://www.youtube.com/watch?v=XqsIAcUyb4E

Learn more at www.proteqc.com

About ProteQC
ProteQC is a vendor-independent cryptographic resilience advisory firm helping financial institutions achieve crypto-agility and reduce quantum-era risk. The firm provides training, assessments, strategy development and ongoing advisory support.

About PQShield
PQShield is a post-quantum cryptography (PQC) company creating the global standards and core technologies to power the future security layer of the world's leading organizations. Its quantum-secure cryptographic solutions work with companies' legacy systems to protect sensitive data now and for years to come. It is the only cybersecurity company that can deliver high-quality

secure implementations of quantum-safe cryptography on chips, in applications, and in the cloud, and is also an authority on PQC side channel attack resistance, having built a dedicated PQC SCA test lab with industry partners. PQShield is also a leading contributor to the post-quantum cryptography standardization projects throughout the world.

Headquartered in the UK, with teams throughout Europe, the United States and Japan, PQShield is principally backed by Addition, Oxford Science Enterprises (formerly OSI), Kindred Capital, Crane Venture Partners, and InnovateUK. Its extensive research paper catalog is available here.

Ana Perez Quiles, Chief Marketing Officer
ProteQC
+1 281-400-3161
press@proteqc.com
