BANK POLICY INSTITUTE

Haunted by Quantum Computing? Face your Fears with the BITS Quantum Risk Calculator

Andrew Kennedy | Oct. 31, 2022

October is renowned for being the scariest time of the year and for good reason. The nights are longer, the days are colder and there is a pretty good chance you aren't going to be the only one dressed up as your favorite superhero at that Halloween party.

And while app-based streams of campy horror films may give some of us quite the fright, for cyber enthusiasts, I dare say something else more sinister is on the far-off horizon. But it is coming. It is coming for us all!

This horror is formless, daunting and irrepressible. We can't see it, touch it or feel its presence, but when it is upon us our understanding of known physics will be forever altered!

What could possibly inspire such palpable fear in the hearts of cyber defenders? Nothing other than the **END**… That is, the end of classic computing and the ushering in of a novel set of risks (and opportunities!) in a post-quantum computing (PQC) world.

But we, in financial services, are risk managers by nature. We don't shy away from a challenge. We embrace it. We identify, analyze and control risk. We game plan every possibility and limit potential downside impact.

Just because something is scary doesn't mean we are paralyzed with fear.

And in the spirit of proactive risk management practices, BITS-BPI is re-launch the Quantum Risk Calculator (QRC).

The QRC is a tool designed to help any person or company better understand how a post-quantum computing future may impact data and applications reliant on cryptography such as encryption, hashing and signatures.

We originally launched this tool in 2018, and this year have made numerous enhancements, simplifications and updates to the recommendations so that organizations have current information at their fingertips.

The tool requires four questions to be answered, so some quick research may be required.

- How long must your data be secured? Typically, this can be answered by regulatory statute or company policy.
- How long would you estimate the change control process to take for the application or data? Think about how long it took some firms to be fully prepared for Y2K.
- When will Quantum Computing become mainstream? This is a best guess as no one knows the correct answer just yet. If you are unsure, consider estimating large-scale quantum computing becoming available by 2031.

- And lastly, what sort of encryption is being used? Symmetric or Asymmetric.

Further information about how to best answer these questions can be found by clicking the corresponding buttons via the web app.

Using these four answers, we calculate the immediacy of the problem (if any) and provide short- and long-term ideas about how to manage the issue and ultimately mitigate the risk going forward. Finally, we will offer you the opportunity to save a PDF of the results for your records (don't worry, we don't save any identifying data on our side — all calculations are anonymous).

Now instead of being haunted by a PQC world, you can prepare for it. Instead of hoping the problem is too far off, you now know when action needs to be taken. Instead of thinking the problem is intractable, now you can build a strategy to reduce your risk.

Should Quantum Computing keep you up at night? Take the challenge by visiting https://quantum.bpi.com/ **from any web browser or mobile device.**

Disclaimer: The views expressed do not necessarily reflect those of the Bank Policy Institute's member banks, and are not intended to be, and should not be construed as, legal advice of any kind.