Coming Healthcare Cyberattack Crisis: Quantum Computing

By Steve Foster

Steve Foster is a lead cloud security architect for TIAA. He has more than 20 years of industry experience with multiple certifications including Certified Systems Security Professional, Certified AI Expert, Amazon Web Services, Microsoft, Blockchain and Agile.

TIAA collaborates with the Health Information Sharing and Analysis Center (Health-ISAC) in sharing cybersecurity thought leadership and best practices.

In this blog he focuses on the quantum computing technology wave and its impacts on cybersecurity, generative artificial intelligence (AI), and the healthcare industry. He'll also offer steps healthcare professionals can consider taking to help avoid quantum-computing-powered cyberattacks, and skills they can develop to strengthen cybersecurity.

Problem statement

The healthcare industry, already facing widespread cyberattacks, shortages of cybersecurity workers, and possessing a vast amount of sensitive patient data, has another major problem coming its way: quantum computing.

This unbelievably fast technology – some estimates put the computational speed at 158 million times faster than today's fastest supercomputers -- has the potential to overpower and break through legacy encryption technologies used to prevent healthcare industry cyberattacks.

As such, quantum computing is prompting the need for post-quantum cryptography that could produce new algorithmic ways to fend off this formidable technology.

But there's more complexity to this situation. The rapid proliferation of generative AI, quantum computing and post quantum cryptography will also impact cybersecurity.

This article will focus on these converging technology-based trends through the larger context of the healthcare industry which is now severely challenged by cyberattacks. An ISC2 report titled "How the Economy, Skills Gap, and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce 2023 revealed that 79 percent of healthcare professionals, the highest among 23 industries and that the current cyberattack threat landscape is the most challenging it's been in five years.

Healthcare security professionals can become more prepared for quantum computing and related cyberattacks and pursue new cybersecurity strategic plans and investments.

What is quantum computing?

A simple way to understand quantum computing and its power is this: the technology can perform an enormous number of mathematical computations simultaneously. Current encryption technologies can only execute these mathematical computations sequentially, which means they're much slower. Simply stated, simultaneous math beats sequential math. Quantum computing's faster math overpowers the slower math processing used in modern encryption. This all points towards more cyberattacks.

What's is post-quantum cryptography?

What can be done?

The answer is the creation and use of post-quantum cryptography (PQC), a replacement for current public key cryptography. Industry leaders are focused on developing new algorithms designed to strengthen encryption so it can fend off quantum computing cyberattacks against healthcare institutions and many other industries.

Big intersection: quantum computing and generative AI

Generative AI directly relates to this quantum computing trend from a cybersecurity perspective. A breakthrough technology that hit the market in 2022, generative AI enables people to type in prompts online and generate text, graphics and video in seconds – at astounding speeds.

When you combine generative AI's blazing speed with that of quantum computing, the result is an amplification of the rate and power of cyberattacks, making it easier and faster for bad actors to create more convincing phishing, deepfake and other harmful cyberattacks.

Viewed through a more positive lens, the computational speed of quantum computing could improve the accuracy, efficiency and speed of the machine learning that powers generative AI which could help cybersecurity professionals more accurately and quickly detect cyberattacks and, for instance, patch vulnerabilities faster.

Overall market impact

Taking all this into consideration, one point is clear. The quantum computing market is on the rise. Spherical Insights research shows the market is expected to expand 26 percent each year and reach $143 billion by 2032 – a huge rise from $13.67 billion in 2022. Industry experts have been sharing insights on how impactful quantum computing will be on generative AI and cyberattacks.

"If you were surprised by the massive leap forward when generative AI emerged in late 2022, you should expect that a possibly bigger jump forward in AI will happen when quantum and AI intersect in our not-too-distant future," according to SDX Central.

Capturing a similar tone, Silicon Republic reports that transitioning to quantum-resistant cryptography this year will become a "mainstream boardroom discussion. No longer a buzzword or a topic to be tabled, becoming crypto-agile to prepare for post-quantum encryption will be a key focus for the C-suite next year."

Specific threats to healthcare

Quantum computing has the potential to have major impacts on the sophistication, volume, and harm cyberattacks inflict on the healthcare industry. For example, various types of medical Internet of Things (IoT) devices such as continuous positive airway pressure (CPAP) machines will be especially vulnerable. Also, currently encrypted medical information, if not properly updated with stronger algorithms and hardware that supports the latest algorithms, may also become accessible to those with malicious intent.

And bad actors will be able to use quantum computing to decrypt healthcare finance transactions, sensitive patient/doctor emails, and patient records, in seconds. Healthcare communications and sensitive data on virtual private networks, browsers, and on cloud computing networks will also be vulnerable to quantum computing cyberattacks.

Data harvesting

There's another challenge. Cyberattackers who steal data from healthcare organizations now are holding on to encrypted data until quantum computing can decrypt it, even if they have to wait several years.

And specifically, quantum computing has the potential to increase the number and effectiveness of the several types of cyberattack threats including four of most prevalent in healthcare: phishing, ransomware, data breaches, and distributed denial of service attacks.

Upside to this story

As harmful as it could be, the power of this technology could benefit healthcare professionals. There could be faster development of new vaccines and drugs, earlier and more precise diagnosis and prediction of diseases such as cancer and Parkinson's, and more preventative versus reactive healthcare. Technologies as powerful as quantum computing, especially combined with generative AI, can help detect and prevent cyberattacks against the healthcare industry faster and more efficiently.

Roadmap to mitigate quantum cyberattacks

What can you do about all this? Plenty, it turns out. Steps you can consider taking to bolster your healthcare organization's cybersecurity were shared by TIAA's during April's Health-ISAC Webinar hosted by TIAA's Steve Foster. He delineated the steps into two categories: planning and execution.

From a planning perspective, he suggests healthcare security professionals expand existing standards and policies to include more quantum-resilient algorithms and processes. He also points out that work hours and technology to fully shift to a PQC organization will be costly and potentially take several years. Leaders in charge of funding these quantum computing cybersecurity programs should be engaged early and provided cost risks of not taking action.

In terms of execution steps, he suggests migration of systems that cannot be enhanced with stronger algorithmic methods to parts of the network less accessible to lower the number of openings to cyberattacks. It's also crucial to embrace a resilient mindset with the flexibility to redirect efforts based on new data.

Skills to develop

Healthcare cybersecurity professionals will strengthen their abilities to withstand quantum computing cyberattacks by developing or sharpening several skills. A few of the most valuable are detailed below.

Convergence of quantum computing, AI, and cybersecurity

Beyond the foundational skills expected to be needed in many tech industry jobs -- proficiency in physics, engineering, math, computer science, software engineering, and software programming -- you'll want to develop a strong understanding of the inter-

related fundamentals of quantum computing, cybersecurity, and AI. Comprehend how quantum computing impacts generative AI in launching and preventing cyberattacks. You'll be more valuable if you can more effectively use tools and technologies associated with all three technologies.

Post quantum cryptography

Developing skills using PQC will position you well. This involves familiarizing yourself with the latest algorithms approved by the National Institute of Standards and Technology that are so mathematically complex they can withstand quantum computing's encryption-breaking computational speeds. As part of this, it will be particularly valuable to become knowledgeable and start using new PQC algorithms that NIST is now developing for preventing quantum computing from breaking the next generation of encryption.

NIST chose four algorithms for post-quantum cryptographic standardization designed to execute two main encryption tasks: general encryption used to protect information exchanged across a public network, and digital signatures used for identity validation.

"If you do not use these algorithms, then you'll eventually be vulnerable to threats from quantum computers that would completely break some of the crypto-systems we use today," said Dustin Moody, NIST's post-quantum cryptography project lead, in a SDXCentral article.

Quantum computing keys

Two additional skills will enhance your value: gaining knowledge of, and developing the ability to use, quantum computing keys because they're pivotal for protecting data from quantum computing cyberattacks.

Python

Start developing or sharpening your Python software programming language skills. The format and structure of the language which is commonly used within the realm of AI/ML today provides a framework that can be upskilled to languages such as Quipper designed to be used within the realm of quantum computing.

Future insights

It’s important to start preparing now for the coming wave of quantum computing to protect healthcare professionals and institutions from cyberattacks aimed at stealing sensitive data and money and disrupting the entire system. Along the way keep in mind that while the threats are real and could be enormous, there are benefits you could gain from using this technology.

“The race is on to develop quantum-safe encryption and harness quantum computing for cybersecurity before it's too late,” according to this LinkedIn article. “With diligence and the right investments, the good guys could gain the upper hand.”