Is your organization quantum ready?

Something that makes companies nervous is uncertainty about the future. To lower future uncertainty companies plan, budget, address trends (and their implications) or try to anticipate the future. They engage in strategic conversations by looking forward.

So what technologies will disrupt the marketplace and how can companies prepare? A paramount issue will relate to privacy and data security which we need to plan for.

A technology that is becoming practical is quantum computing. Although quantum computing has been around for many years, the practicality of it is beginning to be realized. To understand this largely unknown technology, it may help to watch reruns of Quantum Leap, a science fiction show about traveling through time. Andrew Cheung, CEO of 01 Communique Laboratory Inc. based in Toronto noted, “My reaction was similar to many people. I said to myself, “Spock in Star Trek talked about that when I was 10 years old. “This is just a fiction.” Well, this is true until about 2 years ago when the development from the like of D-Wave, IBM, etc. had evolved beyond fiction.”

What is quantum computing? The term might sound scary or almost impossible to understand. However, its implications need to be understood by leaders and decision makers, especially by organizations where data exchange is core to their business model.

Quantum computing is based on the laws of quantum mechanics which allows computers to process information much faster than the current computer systems. Current computers use bits, the smallest unit of data in a computer, which is either a zero or one. Quantum computing uses quantum bits or qubits to process information. Based on quantum mechanics, qubits can have multiple states at the same time rather than just on/off states (ones and zeros) in a traditional computer. Two important phenomena that make quantum computing innovative are superposition and entanglement. Essentially these two concepts enable computers to perform large number calculations simultaneously. Pre-quantum computers will find this task to be slow or impossible when factors are very large.

Because of the factorization of numbers, quantum computers can be used to solve difficult problems. Cheung notes, “In fact, the Quantum Computer is opening a new chapter for human inventions. Its excessive computing power will open new chapters in the field of DNA study, traffic, routing, chemical reaction, quantum physics, etc. This will inspire a lot of new inventions in mankind.”

However, an important negative implication of this capacity to factor large numbers will render cybersecurity systems obsolete. Credit card information, bank communication, stock exchanges and even block chain technology can be “hacked” by quantum computing. While this can be overcome, leaders and decisions makers must begin to prepare their organizations for this reality.

Modern day organizations secure their communication channels through solutions such as Secure Sockets Layer (SSL), Secure Hypertext Transfer Protocols (HTTPS), and Virtual Private Networks (VPN).These forms of encryption are used to protect the information being exchanged between client computers and merchant servers. An ordinary computer would take years to “hack” the encryption while quantum computing can take virtually seconds to minutes to “hack” existing encryption.

Cheung notes, “We first learned about the development of Quantum Computer about 10 years ago that its excessive computing power will likely post threat to the asymmetric cryptography system (e.g. DSA, ESDSA, etc.), which is the core cybersecurity the world is heavily relying on, including our remote access channel, and the current blockchains.”

Governments and security agencies should be concerned about the power of quantum computing when it hits the marketplace. If quantum computing falls into the wrong hands there could be major geopolitical, economical and security implications. Given the vast amount of information being generated by individuals, the future of data security is at risk. And it is only a matter of time before quantum computing reaches the marketplace.

The good news is that, as of today, the power of quantum computing has not advanced to the point where it threatens cybersecurity. However, leading companies in quantum computing like D-Wave, IBM and Google are predicting that within 3-5 years, quantum computing will be advanced enough to put cybersecurity systems at risk. “The problem is that if we do not react and get ourselves ready now, it will be too late when this happens” says Cheung, whose company has developed a solution to quantum-proof cybersecurity systems.

An effective way to think and plan for the future is to visualize more than one scenario. One scenario is to wait until quantum computing revolution hits the marketplace and then adjust to the changes taking place. Another scenario is to start preparing for the future now. The quantum computing revolution will impact small companies, large organizations and governments all over the world. Is your organization quantum ready?

Dr. Proseku is a freelance consultant and is passionate about technology, strategic foresight and leadership. He can be reached at idlipro@mail.regnet.edu.