Don’t let drivers for quantum cyber readiness take a back seat!

By Colin Soutar, Itan Barmes, and Casper Stap

More and more organizations are becoming aware of the threat that future quantum computers will pose to the cryptography that is used to protect vast amounts of digital data every day. When emerging technology evolves, many organizational leaders rely on regulations as the tipping point for action. Potential regulatory action was deemed one of four drivers in Transitioning to a Quantum Secure Economy, a report by the World Economic Forum, in collaboration with Deloitte. But although regulations will be important guardrails to a future quantum-secure society, organizational IT leaders should not wait for them to arrive and, instead, should act now. Quantum technologies and the resultant threat to cryptography will likely not follow the “normal” linear sequential path for emerging technology as risk emerges and regulations evolve. Read more to understand why.

Let’s begin by untangling the ***threat***. Today’s quantum computers are not able to break cryptography, and this will likely not happen until a so-called Cryptographically Relevant Quantum Computer (CRQC) [see NSA] is available, which many experts believe to be ten to fifteen years away. When this topic is discussed, there is often conjecture about the validity of this forecast, sometimes even including the steps that are needed for a CRQC to materialize. For many organizations, this may cause a delay in the call to action. We prefer to cast this threat in the following manner: Even if you think a CRQC is at least ten years away, do you know with enough confidence that time is long enough to do the required cryptographic updates across your infrastructure? So, the big question really becomes, what do you need to do to start getting ready and, more importantly, how long is a transition to quantum-resistance going to take you?

To exacerbate these timeline issues, different data types are expected to remain secret for different durations. For example, personal information is expected to remain confidential for an individual’s lifetime, national security information is expected to remain secret for decades, but financial transactional data is generally ephemeral. Thus, personal information that is stolen ***today*** and which could be revealed in 10 years is already potentially compromised. It is widely believed that threat actors may already be stealing large amounts of encrypted data in the anticipation that they will be able to crack it open later when a CRQC is available to them –a so-called Harvest Now, Decrypt Later attack.

The steps organizations can take to address the threat of quantum attack are relatively straightforward, albeit an immense task (thus very hard to prioritize alongside other threats). First, they should understand what vulnerable cryptography they currently use, and what data would be affected by a CRQC attack. This is already being required of US federal agencies through Office of Management and Budget Memorandum 23-02. Second, they will then need to implement Post-Quantum Cryptography (PQC), which is designed to protect data from quantum computer attacks.

And here the regulatory dimension kicks in.

As a first step, the US National Institute of Standards and Technology (NIST) has been hosting a global competition for PQC algorithms for the last 8 years, and is expected to publish final standards for quantum-secure cryptographic algorithms by the end of 2024, and has just released initial drafts for comment. Once finalized, these standards for PQC will be published as ***Federal Information Processing Standard (FIPS)*** documents, which contain detailed and technical language on implementation of the algorithms. Such FIPS standards formally apply—as the name might imply—to US government departments and agencies. FIPS documents such as FIPS 140 in cryptography are well-known and internationally recognized and, therefore, serve as de facto standards worldwide.

Depending on global industry response, a next step may be the development of a ***global consensus standard***, such as of the International Organization for Standardization (ISO), although the prescriptive nature of cryptographic standards would hopefully indicate that it would traverse that consensus process without substantive updates.

A subsequent route will be ***guidance documents*** that advise stakeholders on how to embed cryptographic standards into products or protocols. There have already been some initial, and often high-level, guidance documents issued by countries such as US, Germany and France, as well as organizations such as the Internet Engineering Taskforce.

Which brings us to the crux of the issue: It is likely that many of these steps will need to be completed before ***regulations*** are confidently completed, which makes waiting for regulations to fully develop a risky proposition. The FIPSs will have to be finalized and field tested, likely along with some degree of global adoption before regulators will be comfortable incorporating them. While regulations often provide a driver for the adoption of risk-mitigation technologies; with the various timelines at play here, we believe that some of the regulations may evolve too slowly to be effective.

Instead, it's better to act proactively and be ahead of the curve, rather than waiting for regulations to emerge. As noted above, there are several steps that can be taken today, including:

- Conduct ***an organizational cryptographic and data inventory*** to understand your potential exposure;
- Assess that risk alongside other organizational cybersecurity risks, leveraging a progressive ***framework*** such as the NIST Cybersecurity Framework (CSF);
- Develop a roadmap to achieve ***cryptographic agility***—that is the ability to readily interchange or add cryptographic capabilities.

These steps can assist organizations to be poised to adopt standards or respond to regulations in an orderly way. Furthermore, we have experienced that reviewing organizational cryptographic hygiene is never a bad thing. It can often lead to unexpected observations, which can subsequently lead to cybersecurity improvements that may support and accelerate the quantum security journey.

In short: don't wait for potential regulations, and act now on the basic cyber hygiene steps that are always helpful!