



# Fibre Channel Advances Security in a Quantum World

*Barbara Porter – Product Marketing Manager, Broadcom Inc.*

---

Data breaches are becoming more frequent and more expensive. In industries categorized as critical infrastructure – health care, financial services, pharmaceutical, energy, transportation, and industrial – the losses are significantly higher than in other sectors. In 2024, the health care industry experienced the highest average data loss cost at US\$9.77 million per breach, double the average breach cost of US\$4.88M million.<sup>1</sup>

That's worrisome because powerful new quantum computers will bring grave new threats on top of the increasing baseline risk. Cybersecurity experts fear that quantum computers will be able to crack cryptographic algorithms that have long resisted cyberattack by traditional computers.

## The Quantum Threat

Although current computing technology might theoretically be able to solve the math behind current cryptographic solutions, the possibility remains speculative given the prohibitive expense of trying it. It's been demonstrated, however, that quantum computers will be able to solve such complex problems in a fraction of the time.

Quantum computing relies on physics at extremely small scale and at low temperatures to execute an [entirely new category of algorithms](#). "Security" as it is known in the classical computing context is no longer secure.

In response, governments around the world have developed new laws and regulations aimed at modernizing data centers. The Fibre Channel industry has responded with new standards that tighten the security on what is already considered the world most secure – and in fact, air-gapped – network technology upon which critical infrastructures rely for their most valuable data assets.

## The Hack

The [2020 SolarWinds attack](#) spurred governments around the world to initiate a slew of new regulations. By managing to insert malicious code into a SolarWinds software product update, hackers gained access to the networks, systems, and data of thousands of SolarWinds customers, including federal government systems. The company's update of its Orion network monitoring software inadvertently infected 18,000 of its customers. The scope of the hack is unprecedented and is one of the largest ever documented (if not the largest).

## Governments Step In with Zero Trust Architecture Mandates



In response to the SolarWinds hack, the U.S. President Joe Biden on May 12, 2021, issued a Presidential Executive Order to Improve the Nation's Cybersecurity. The order included a mandate that government suppliers modernize their data centers, including adopting the principles of Zero Trust Architecture. The United Kingdom's National Cyber Security Centre (NCSC) issued its own guidance for enterprise environments focused on zero trust concepts. The fundamental tenets of zero trust include authentication between all entities and encryption of all data flows. The essence of zero trust: "Never trust any network,

especially your own.”

A zero trust architecture is defined by seven key tenets, each essential for its effective inclusion in a company’s cybersecurity infrastructure:




## Preparing for a Quantum Future



PRESS RELEASE | Sept. 7, 2022

NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems



Of course, zero trust solutions would be ineffective if they didn't account for the quantum computing threat. Accordingly, in 2022 the U.S. National Security Agency (NSA) issued its CNSA 2.0 requirements, mandating the use of new quantum resistant algorithms (QRAs). This followed up on the initial CNSA 1.0 advisory in 2016, which recommended higher strength classical algorithms until the NSA could complete its quantum resistant algorithm investigation. In parallel, the European Union announced its Cyber Resilience Act (CRA), which mandates common EU requirements for hardware and software.

An essential authority in computing standards is the National Institute of Standards and Technology (NIST), a scientific partner of the NSA. Together, the organizations formulate U.S. cryptographic policy. NIST authorizes suitable encryption algorithms for widespread use by servers and standardizes cryptographic solutions. Original encryption algorithms used in classical computers were once considered very secure, as computers did not have the strength or processing capabilities to decrypt these algorithms. One such algorithm, the most commonly and widely used and accepted form of encryption, is the Rivest-Shamir-Adleman (RSA) algorithm. It is an asymmetric algorithm that ensures a reliable level of confidentiality in the classical computing context. Classical computers simply do not possess the processing capabilities or efficiency required to realistically crack such encryption.

The landscape changed in January 2019 with the introduction of the first fully integrated, circuit-based commercial quantum computer, the IBM Q System One. Five years later, quantum computers are being deployed in universities and research labs and are expected to scale solutions over the next 10-20 years. A cryptanalytically relevant quantum computer (CRQC) is a quantum computer that is theoretically capable of attacking real-world cryptographic systems. A CRQC could possess the ability to decrypt public key (also known as asymmetric key) encryption systems. This is a significant concern among security analysts today, as almost all of today's information systems rely on the asymmetric key method to secure sensitive data. Namely, quantum-performed algorithms, such as Grover's search and Shor's algorithms, pose a significant threat to the RSA algorithm.

The concern that hackers could "catch now and crack later," (i.e. steal and store data now, and decrypt it later with a quantum computer) is real. Think about presumed encrypted messages or files from 20 years ago that would still be relevant today. Even if CRQCs are not available for 20 years, quantum resistant cryptography needs to be deployed now.

NIST has formally released standards to cover all major cryptography needs. It is widely believed that the EU, and most of the rest of the world, will adopt the CNSA algorithm suite.

## Governments Set Timelines for Quantum Resistant Algorithms

So where does this new cryptography stand today? The timeline for CNSA and ENISA (European Union Agency for Cybersecurity) compliance requirements is coming up fast. In 2025, shipments of IT equipment into the U.S. government are recommended to include CNSA 1.0 or 2.0 components. In 2030, shipments are required to include CNSA 2.0 components. In 2026, ENISA expects Quantum Resistant algorithms to be adopted.

NIS 2 (Network and Information Systems Directive) in the EU also has important upcoming deadlines. By October 2024, enterprises need to adopt and publish measures intended to improve the security of network and information systems across the EU. The EU's Digital Operations Resilience Act (DORA) will by 2025 require compliance with legislation to improve the IT security of financial institutions and their third-party service providers. The urgency continues to build as governments around the world enact new security compliance regulations and enterprises must be ready.

## Encryption of Data In-flight on Fibre Channel Networks

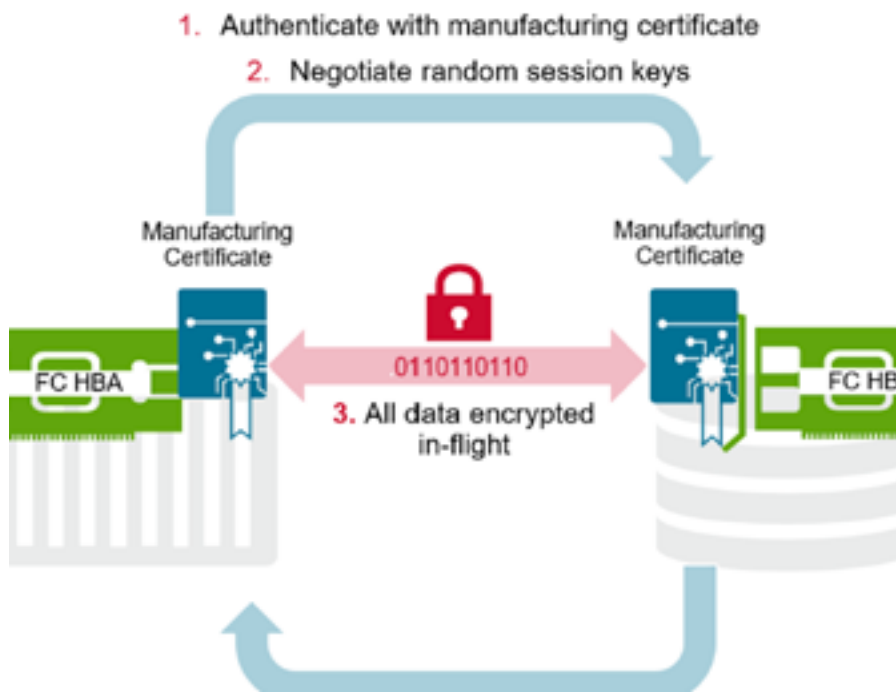
The focus of concern that drives all of these government-led initiatives is to protect critical infrastructure, the value of which was revealed in the pandemic. As the preferred storage solution for mission-critical data center solutions, Fibre Channel must take the lead in post-quantum and zero trust solutions.

The new Fibre Channel SP3 (FC-SP-3) standards support authenticated encryption of data in flight (EDIF) using quantum resistant algorithms. The new algorithms are incorporated into FC HBAs starting in 2025 for both servers and storage. This allows fibre channel SANs to both meet zero trust requirements as well as CNSA timelines for quantum resistance.

Once ratified, FC-SP-3 will enable governments and enterprises to comply with CNSA 2.0 mandates ahead of the required 2025 and 2030 deadlines.

The goal of FC-SP-3 was to deliver an open, easy to implement solution that made it easy for enterprises to comply with CNSA mandates. Research shows that in 2023 organizations with high levels of security system complexity reported a US\$1.4M increase in data breach cost over organizations with low system complexity.<sup>1</sup> The FC-SP-3 solution solves the encryption complexity problem. The solution involves

manufacturing certificates stored on Fibre Channel Host Bus Adapters (HBAs) authenticating as valid and, once identities are established, negotiating random session keys. All data is then encrypted in flight between the servers and storage arrays. A huge benefit of this approach is that it uses session-based keys and does not require a complex external key management application, making it very easy to deploy and manage.



**Figure 1: Fibre Channel EDIF - Session-based Encryption**

The solution is also cost-effective. It can run on an existing Fibre Channel network without new hardware (apart from deploying HBAs that support FC-SP-3).

Unlike application-based encryption, where individual applications implement their own encryption schemes, Fibre Channel encryption encrypts all data in flight, providing complete coverage for all apps at a lower cost. It also has no impact on storage array features such as compression and deduplication.

Compared to general purpose Ethernet (IPSEC) adapters, modern Fibre Channel HBAs have dedicated hardware offload for crypto functions to avoid degrading performance and provide simple management.

The FC-SP-3 standard is expected to be completed in 2025 with both server and storage solutions available in the marketplace that same year.

## Completing Fibre Channel Zero Trust Solutions

Zero trust architecture requires continual authorization, requiring establishment of trust at every possible digital interaction. This approach acknowledges that threats can come from inside and outside the network. Fibre Channel vendors have implemented, or will be implementing, zero trust components which may include:

Silicon Root of Trust- uses unalterable hardware- based on signature validation to ensure authentic ASIC and firmware.

Digitally Signed Drivers- verified by the operating system to be authentic code written by the manufacturer before they can be installed.

SPDM (Security Protocol and Data Model) - cryptographically authenticates Fibre Channel HBAs with host CPUs.

## Conclusion

Cybersecurity is a focal point of enterprises and governments globally, as the frequency and cost of data breaches continue to rise and the quantum computing era grows nearer. To address these concerns, governments have responded with regulations such as CNSA 2.0, NIS and DORA, mandating enterprises to modernize their IT infrastructures.

New Fibre Channel standards deliver a cost-effective, easy-to-manage solution to meet compliance requirements with support for Zero Trust and EDIF to protect data as it moves across databases, applications, servers, and storage. Fibre Channel HBAs supporting FC-SP-3 utilize quantum-resistant algorithms, ensuring post-quantum readiness. The session-based key management solution does not require complex and costly key management software. Compared to other encryption methods such as application-based encryption and Ethernet IPSEC, Fibre Channel HBAs can encrypt all applications, at a lower cost, and with no impact on storage array services such as dedupe or compression. Considering this will be done with no performance impact, FC-SP-3 based fibre channel solutions will play a pivotal role in protecting critical infrastructures.

---

1. Ponemon Institute, Cost of Data Breach Report, 2023, IBM Security