IronCAP™ Post-Quantum Cybersecurity

Summer - 2025

Tomorrow's Cyber Security, Today

IRONCAP

Disclaimer

Certain statements in this presentation may constitute “forward-looking” statements which involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of the Company, or industry results, to be materially different from any future results, performance or achievements expressed or implied by such forward-looking statements. When used in this presentation, such statements use such words as “may”, “will”, “expect”, “believe”, "anticipate", “plan”, “intend”, “are confident” and other similar terminology. Such statements include statements regarding the Company’s ability to grow revenues and margins, the business prospects of IronCAP X™, the future of quantum computers and their impact on the Company's product offering, the functionality of the Company's products and the intended product lines for the Company's technology. These statements reflect current expectations regarding future events and operating performance and speak only as of the date of this presentation. Forward-looking statements involve significant risks and uncertainties, should not be read as guarantees of future performance or results, and will not necessarily be accurate indications of whether or not such results will be achieved. A number of factors could cause actual results to differ materially from the matters discussed in the forward-looking statements, including, but not limited to, a delay in the anticipated adoption of quantum computers and a corresponding delay in Q day, the ability for the Company to generate sales, and gain adoption of, IronCAP X™, the ability of the Company to raise financing to pursue its business plan, competing products that provide a superior product, competitors with greater resources and the factors discussed under “Risk and Uncertainties” in the company’s Management`s Discussion and Analysis document filed on SEDAR. Although the forward-looking statements contained in this presentation are based upon what management of the Company believes are reasonable assumptions, the company cannot assure investors that actual results will be consistent with these forward-looking statements. These forward-looking statements are made as of the date of this presentation, and the company assumes no obligation to update or revise them to reflect new events or circumstances.

This presentation contains statistical data, market research and industry forecasts that were obtained from third party web sites, publications and reports or are based on estimates derived from such publications and reports and the Company’s knowledge of, and experience in, the markets in which it operates. The third party publications and reports generally indicate that they have obtained their information from sources believed to be reliable, but do not guarantee the accuracy and completeness of their information. Actual outcomes may vary materially from those forecasts in such publications or reports, and the prospect for material variation can be expected to increase as the length of the forecast period increases. While the Company believes this data to be reliable, market and industry data is subject to variations and cannot be verified due to limits on the availability and reliability of data inputs and other limitations and uncertainties inherent in any statistical survey. Accordingly, the accuracy, currency and completeness of this information cannot be guaranteed. The Company has not independently verified any of the data from third-party sources included in this presentation or ascertained the underlying assumptions relied upon by such sources.

Investment Highlights

What is the Quantum Threat (Q-Day)

- Quantum computers will crack current encryption methods
- Everything is vulnerable: email, financials, crypto, AI, etc.

Q-Day Protection (with US Patents)

- Convert everything to become Quantum-safe
- 01 Quantum is the leader with its IronCAP™ product line

Why Invest Today?

- Quantum-driven cybersecurity threat urgently need solutions today
- World's First Commercial SaaS Quantum-safe Cybersecurity products
- Widely recognized expertise being monetized with global partners

Quantum Computing
A Near-term Commercial Reality

IBM Roadmap
Expects large-scale fault tolerant quantum computer by 2029

IBM 2025-2026 Deliveries
Loon (2025) → Kookaburra (2026)

Quantinuum (Honeywell)
New version within 2025 will be 1 billion times faster

Microsoft
"Majorana 1" topological core in Feb 2025

Google
Willow achieved a major breakthrough in Dec 2024

Q-Day is today's problem

Executive Office of the US President

- Reminded agencies to be mindful that encrypted data can be recorded now and decrypted at a later date by operators of a future CRQC (Cryptanalytically Relevant Quantum Computer).

US Secretary of Commerce (Howard Lutnick)

- The worldwide cybersecurity will be totally broken by quantum computers if we don't act immediately.

Canadian Government

- The Carney government has named quantum technologies as a priority topic in the G7 meeting.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with National Security Memorandum 10 (NSM-10), *on Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).[1]

I. OVERVIEW

Federal agencies[2] ("agencies") are moving to a zero trust architecture, as directed by Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021)[3] and Office of Management and Budget (OMB) Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).[4] This paradigm shift relies in part on the ubiquitous use of strong encryption throughout agencies.

As outlined in NSM-10, the threat posed by the prospect of a cryptanalytically relevant quantum computer (CRQC)[5] requires that agencies prepare now to implement post-quantum cryptography (PQC). Once operational, a CRQC is expected to be able to compromise certain widely used cryptographic algorithms used to secure Federal data and information systems.

[1] Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[2] The term "agency" has the meaning given in 44 U.S.C. § 3502.
[3] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[4] Available at: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[5] Defined as quantum computers that are capable of actually attacking real world cryptographic systems that would be infeasible to attack with a classical computer.

Recognized Global PQC Partners

- 01 is their SME (Subject Matter Expert)
- Partners have global customers with cybersecurity vulnerability
- Revenue pipeline monetization begun

Our Expertise and Products are Commercially Ready

As PQC Expertise for our global partners (Fee + Rev sharing)

- Crypto-ATM Machines
- Cryptocurrencies Protection
- Quantum VPN
- Quantum Digital Identities
- Multi-Signatures

Quantum-Safe SaaS products (Recurring Revenue)

- Quantum Email Security (Commercially ready now)
- Quantum Remote Access (Commercially ready now)
- Quantum AI Marketplace (Commercially ready in 2026)

Revenue Model

As PQC Expertise for our global partners

- We charge engineering fees plus % of the ongoing revenues
- Subject Matter Expert partnerships in place – pipeline for revenues
- Contractual revenue begun

Quantum-Safe SaaS products

- Quantum Email Security: $9.95/month per email address
- Quantum Remote Access: $9.95/month per user
- Quantum AI Marketplace: 10% of the revenue

Partner Activity #1 - Hitachi

Quantum-Safe + Zero Trust

- Remote access tools are 100% quantum-vulnerable
- We make remote access **Quantum-Safe**. The world's first PQC remote access product commercially ready
- Contract announced in June 2025

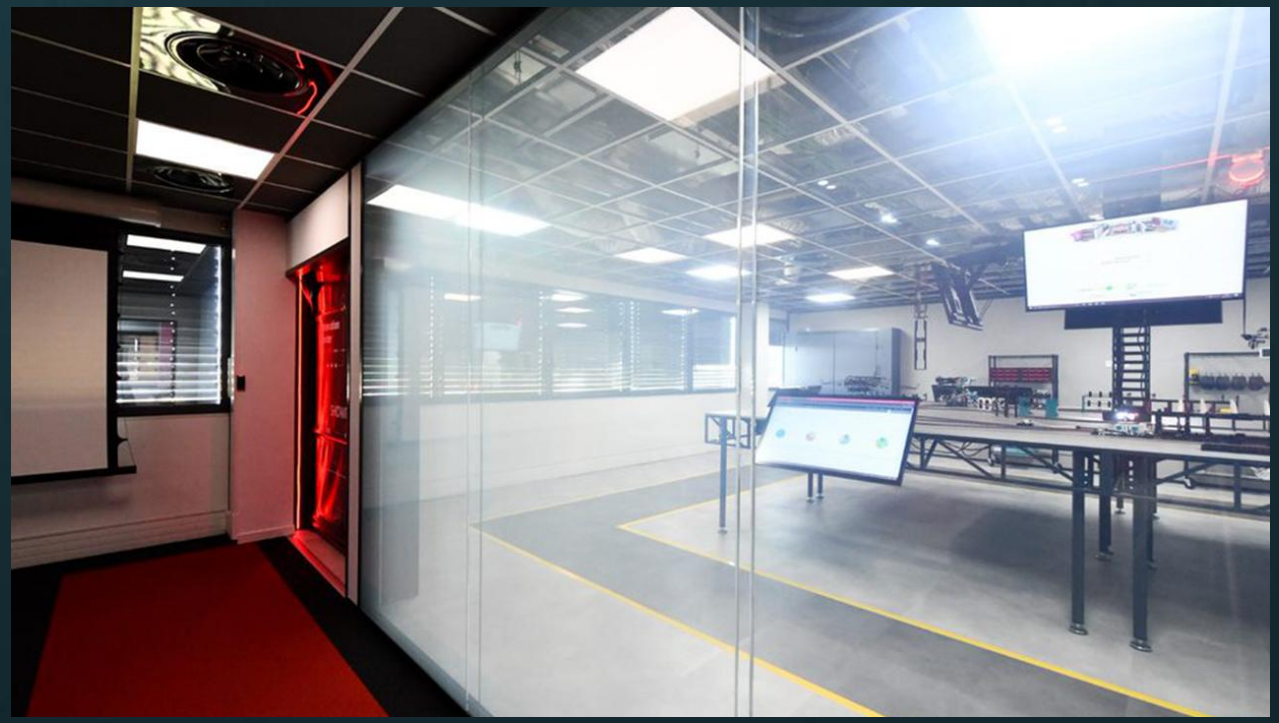
Partner Activity #2 - Crypto

- Every cryptocurrency is quantum-vulnerable (BTC, ETH, SOL, etc.)
- We have patent-protected methods to protect **Existing Public Blockchains** against quantum threat
- Huge market potential: All **$3.4t** of the current cryptocurrency value is at risk unless protected with quantum-safe methods by Q-Day
- Contract announced in July 2025
- One-time development fees + revenue sharing of token sale + % of the founders' pool tokens

Partner Activity #3 - CGI

IronCAP Demo

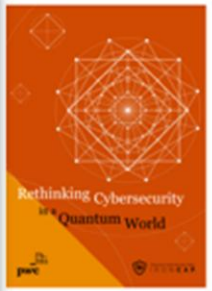
https://ironcap.ca/demo/cgi/



Partner Activity #4 - PwC

pwc

Tomorrow's Cyber Security, Today
IRONCAP



Rethinking Cybersecurity in a Quantum World

https://www.pwccn.com/en/issues/cybersecurity-and-privacy/rethinking-cybersecurity-in-a-quantum-world-jul2021.html

Email Phishing Culprit behind Ransomware

https://www.pwccn.com/en/issues/cybersecurity-and-privacy/email-phishing-culprit-behind-ransomware-apr2022.html

Partner Activity #5 – Crypto ATM

Digital Asset Exchange Machine

We helped a customer in Hong Kong to launch the world's first quantum-safe DAEM at Cyberport in Hong Kong. DAEM

DAEM adopts 2 layers of authentication to ensure end-to-end security between:

1. User's device and DAEM.
2. DAEM and the host application.

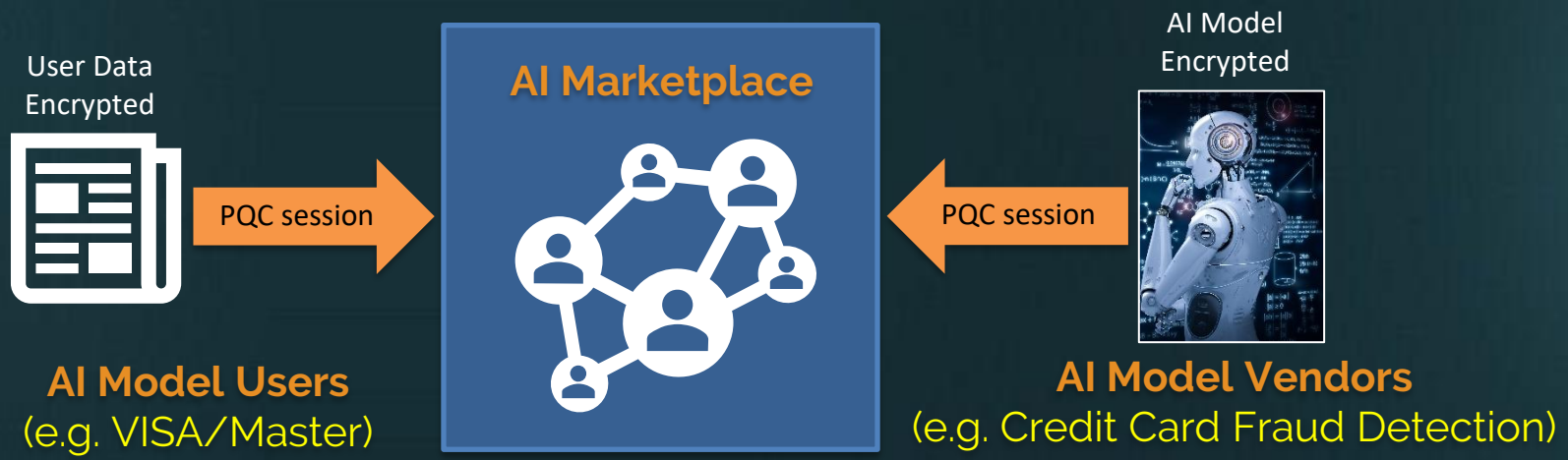
IRONCAP

Email Security – IronCAP X™

https://ironcap.ca/ironcap-x/

- Email is the most widely used business tool in the world but yet 100% quantum-vulnerable
- Emails are 91% the source of ransomware attacks
- We make emails **Quantum-Safe**. The world's first PQC email security product commercially ready
- 730m business emails in the world (10% = 73m)
- Integration with Office Outlook

AI Safety: AI Marketplace



- All AI operations are 100% quantum-vulnerable
- The world's first Amazon-like **Quantum-Safe** marketplace for AI models
- Encrypting confidential user input and AI model (**Zero-Trust**)
- Huge **$3.4t** market potential (**Commercially Ready 2026**)

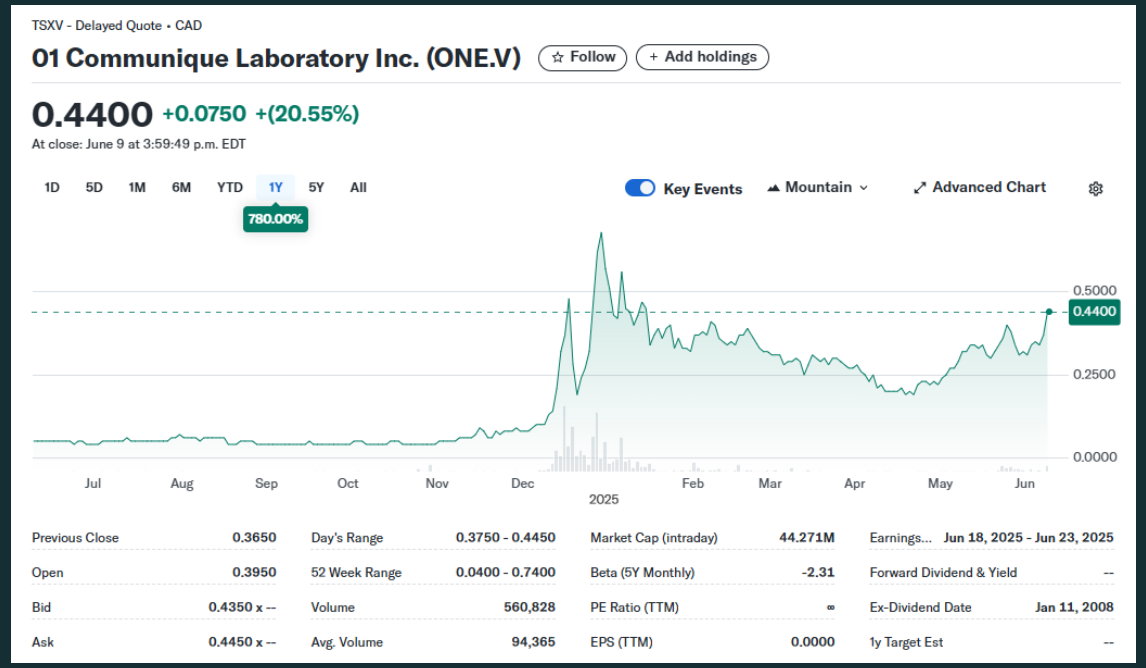
01 Quantum

(TSX-V: ONE | OTCQB: OONEF)

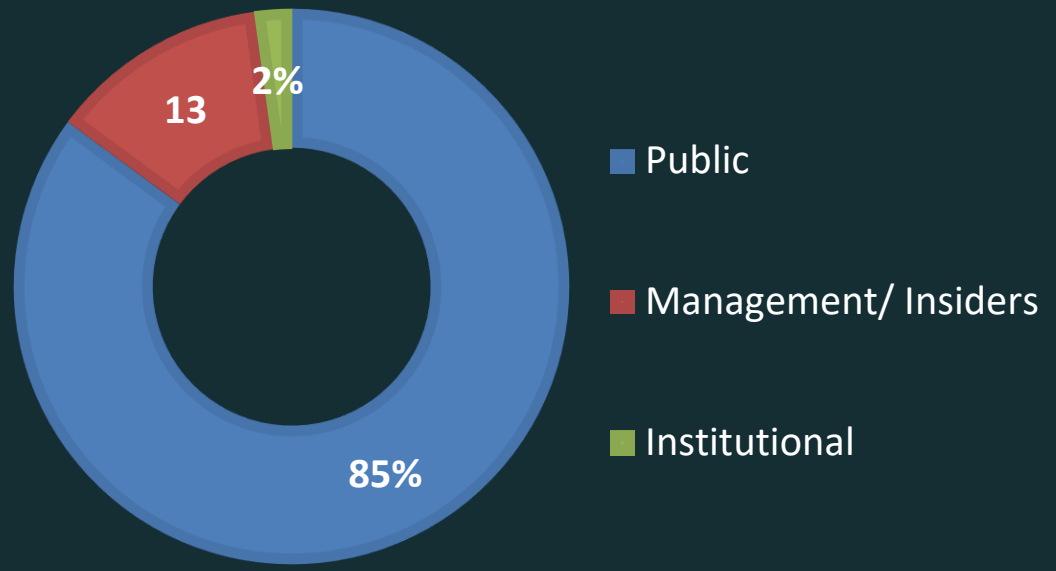
Description	Amount
Market Cap	$45,000,000
52 Weeks High/Low	$0.74 / $0.04
Cash / Debt	$1.2m / $0

Description	Amount
Basic Shares Outstanding	102,319,554
Options/Warrants Outstanding	6,705,000 / 4,852,500
Cash burn (quarterly average)	$200,000

Stock Chart



Ownership Summary



IRONCAP

Management and the Board

Andrew Cheung

President/CEO

Brian Stringer

CFO

William Train

Chairman & Board Member

Gary Kissack

Board Member

Tyson Macauley

Board Member

Professor Edoardo Persichetti

PQC Advisor

The Time to Act = NOW

- The quantum market today = AI market 2 years ago
- Quantum Threat must be protected today
- Revenue tipping point
- The world's first company with quantum-safe products ready to generate recurring revenues
- Subject Matter Expert relationship with our global partners are well established and being monetized

Take Away:

- Quantum Threat is here
- Everything is vulnerable
- Need to act now
- IronCAP is the Solution