

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.



Investor Summary (Winter 2021)

- Quantum Cybersecurity Threat is Arriving
- Proven Patent-Protected Quantum-safe Technology
- Multi-billion-Dollar Untapped Market
- Endorsed by World-class Partners
- Financial Inflection Point



Tomorrow's Cyber Security, Today

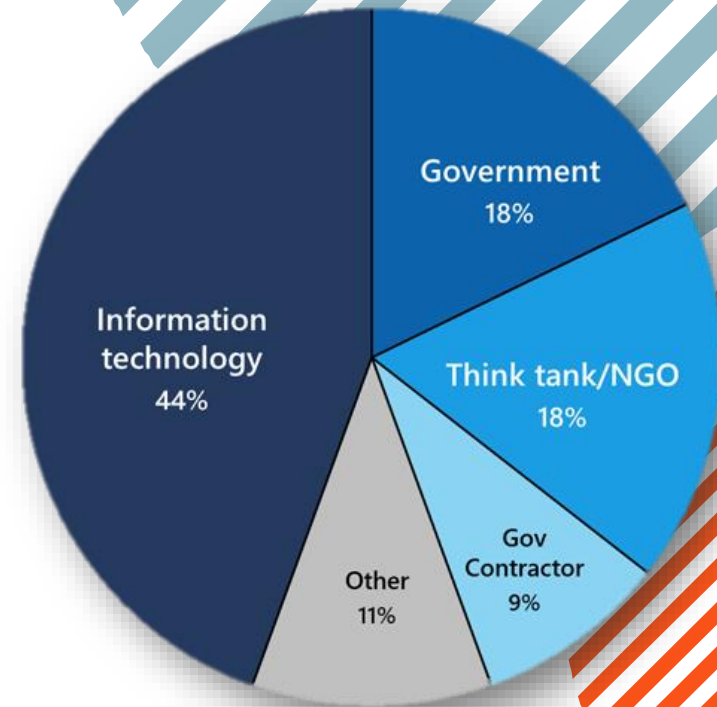
I R O N C A P

(TSX-V: ONE | OTCQB: OONEF)

Cyber Threats **On The Rise**

- ❑ Darkside attacked Colonial Pipeline disrupting critical oil delivery infrastructure and heightened global oil price volatility.
- ❑ Bombardier suffered a massive data breach in Feb 2021
- ❑ Irish Healthcare system has been hacked **twice** in May 2021
- ❑ The average cost of downtime is 24 times higher than the average ransom amount requested

The **world** is being hit by a tsunami of cyber attacks and the winds are only going to get stronger with the fast-approaching quantum computing era.



Cyber Threats **On The Rise**

57% of organizations experienced a successful phishing attack in 2020
- Proofpoint

A new ransomware attack is expected to hit a business every 11 second in 2021
- Cybercrime Magazine

Ransomware attacks cost an average of \$4.62 million (more than the average data breach costs)
- IBM

"Cyberattacks are now the foremost risk to the global financial system, even more so than the lending and liquidity risks that led to the 2008 financial crisis."
- U.S. Federal Reserve Chairman, Jerome Powell,



Quantum Threat is Here

Quantum Computers are commercially available

- IBM released Q in Jan 2019
- Google Sycamore claimed Quantum Supremacy in Oct 2019
- Amazon launched Braket quantum service in Dec 2019
- Honeywell predicted x10/year June 2020
- UST of China released JiuZhang-2 in October 2021

"Quantum Race" between the open and the closed world

- Open world: IBM, Google, Honeywell, D-Wave, etc.
- Closed world: Billions have been invested by many nations

Grab-and-wait strategy presents serious threat

- Hackers seize data and incubate it pending future attack





Tomorrow's Cyber Security, Today

IRONCAP

Experts on Quantum-Safe Standard Readiness

"We think quantum computing is in the future and is a future risk. The reality is that every and each document that is stored today somewhere on a system for a financial institution is actually a potential document that is under attack."

- Florin Philip, Director at CGI Innovation Center Montreal

"However one thing is for sure that everyone is realizing that the Q-day might have already occurred. It just that it is now coming and because a breach that could have happened or a database which is encrypted but lying somewhere there as soon as that readiness or availability of technology comes into the hand of these adversarial players that is going to explode multi-fold."

- Asif Qayyam, Managing Director PwC (Canada)



Tomorrow's Cyber Security, Today

IRONCAP

Expertise at **IronCAP**



Andrew Cheung: CEO

- 25+ years in communications, mobile, and cyber security
- Nominee of E&Y Entrepreneur Of The Year award in 2001
- 7 patents co-invented + several patent-pending applications
- B.Sc. (Hon) degree in Computer Science from the UWO



Sergey Strakhov: CTO

- 20+ years experience in cyber security and cryptography
- 2 patents co-invented + several patent-pending applications
- M.Sc. in Engineering for Computer Systems from the St. Petersburg State University of Aerospace Instrumentation



Professor Bezzateev: Crypto Scientist

- 35+ years experience in cryptography and error correction
- 10 patents co-invented + 100 academic papers authored
- Head of Information Security (IS) Technologies Department at the St. Petersburg State University of Aerospace Instrumentation





Tomorrow's Cyber Security, Today

IRONCAP

IronCAP the Solution



Patent-Protected Innovative Technology

- ❖ Years of R&D with millions invested to create patent-protected, best-in-class, first-to-market, quantum-safe encryption technology



Proven Technology

- ❖ Built on the 50-year time-tested Goppa code-based cryptography theory which has no cracking theory
- ❖ Survived 2 global hackathons in 2019-2021



Seamless Integration

- ❖ IronCAP is compliant with the OpenSSL, PKCS#11, and OpenPGP industry standards that can be seamlessly integrated into existing PKI infrastructure





Tomorrow's Cyber Security, Today

IRONCAP

Addressable Market



Financial Transactions

- ❖ E.g. 2b credit cards VISA/Master combined
- ❖ \$1 per year = **\$2b per year**



Email Security (stop phishing)

- ❖ 730m active business email accounts globally
- ❖ \$10 per year = **\$7.3b per year**



Website Security

- ❖ 170m active websites globally
- ❖ \$10 per year = **\$1.7b per year**



Cryptocurrency Security
Remote Access Security
IoT Devices Security
Digital Identity





Tomorrow's Cyber Security, Today
IRONCAP

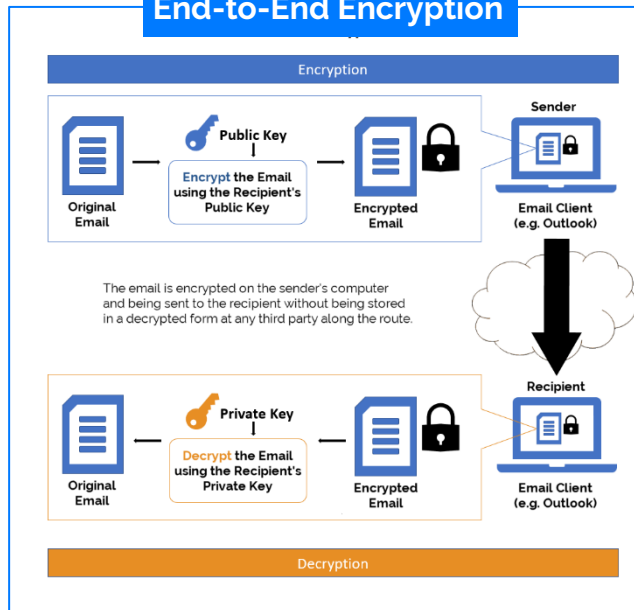
IronCAP X™ Email Security



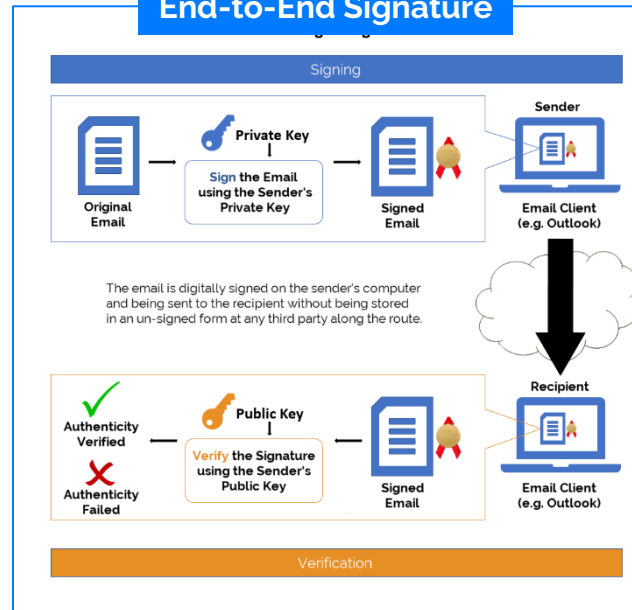
End-to-End Security + Quantum-safe

- ❖ Launching in the Fall 2021 (\$10/yr per user)
- ❖ 730 global business emails (\$7.3b/yr market)

End-to-End Encryption



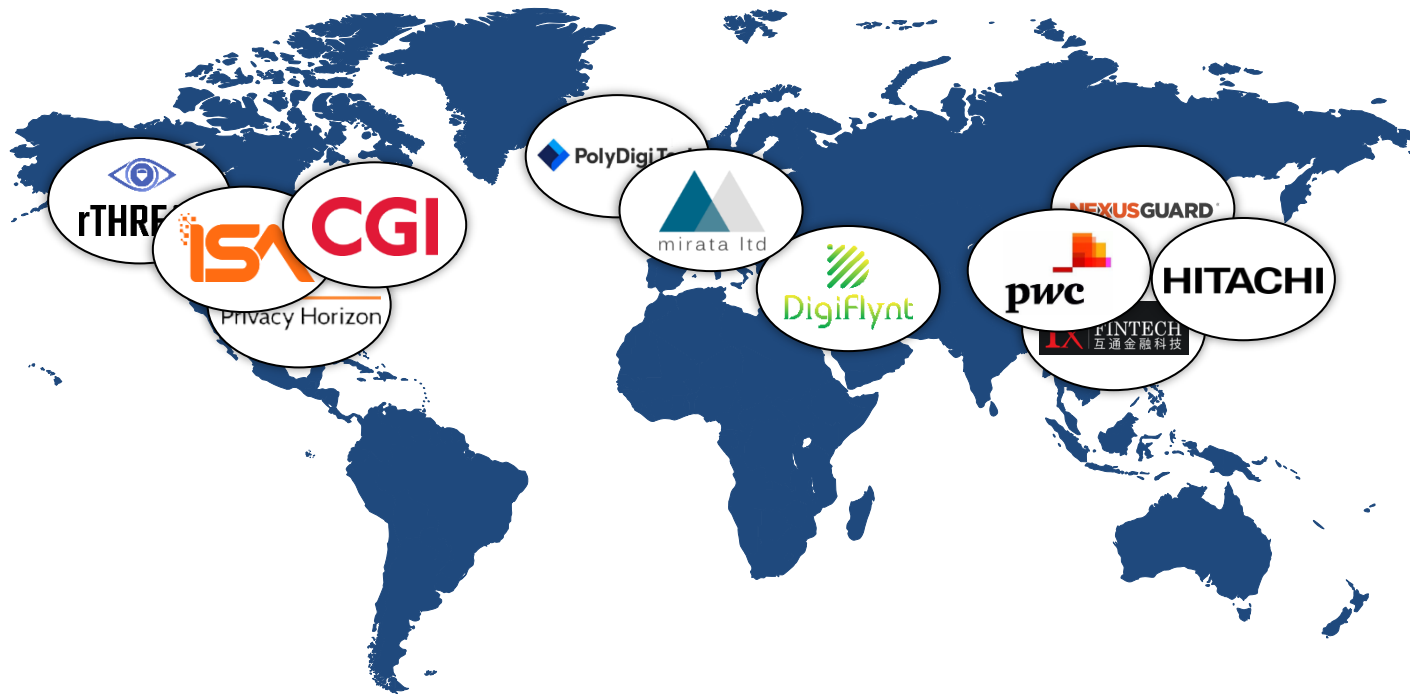
End-to-End Signature





Tomorrow's Cyber Security, Today
IRONCAP

Partnerships ... and expanding



Financial (C\$) Capital Structure

Fully Diluted Shares	100m	Cash	\$1m
Market Cap (in MM)	\$30m*	Debt	\$0
52 Week High/Low	\$0.42 / \$0.12	R&D Invested	\$5m

Stock Chart



Market Cap (USD) Comparison

Fully Diluted Shares	100m
Market Cap (in USD)	\$25m
52 Week High/Low	\$0.35 / \$0.17

Vertical	Name	Market Cap	Notes
Crypto Engine	Arqit	\$2,700m	Nasdaq
Email Security	Mimecast	\$5,000m	Nasdaq
Email Security	ZIX	\$500m	Nasdaq
Website Security	RSA	\$2,000m	Acquired (Mar/2020)
Remote Access	LogMeIn	\$4,300m	Acquired (Aug/2020)



Timing is Everything

Technology Leader

- ❑ Patent-protected and Commercially available
- ❑ Cybersecurity is front and center of every business
- ❑ World's first true quantum-safe end-to-end email security

Financial Inflection Point

- ❑ Perfect timing before massive growth or being acquired
- ❑ Ready to roll out globally with partners
- ❑ Free-riding the trustworthy due diligence: CGI, PwC, Hitachi
- ❑ Cash burning stage behind us

