Francis Bellido on Quantum eMotion’s commitment to innovation in quantum-based cybersecurity solutions

written by InvestorNews | February 27, 2024

In a recent interview with Tracy Weslosky, Francis Bellido, President, CEO, and Director of Quantum eMotion Corp. (TSXV: QNC | OTCQB: QNCCF) shared insights into the significant advancements in the creation of their first Quantum Random Number Generator (QRNG) on a microchip. Highlighting the successful miniaturization of their quantum technology, Francis explains how this microchip offers possibilities for embedding quantum-enhanced security features directly into medical devices, consumer electronics, IoT devices, and other digital systems making them nearly ‘unhackable’.

---

eResearch Industry Report Focuses on Roll-Up Strategies in the Canadian ICT Industry and Features CISCOM Roll-Up

Strategy

written by Tracy Weslosky | February 27, 2024

The recent eResearch Industry Report titled Roll-Up Strategies in the Canadian ICT Industry; Your Guide to Understanding and Investing in M&A-Focused Public Companies offers a comprehensive analysis of the Mergers and Acquisition (M&A) strategies in the Canadian Information and Communication Technology (ICT) sector. This sector, pivotal in modern business and society, includes key components like cybersecurity, data management, and telecommunications. Despite challenges posed by COVID-19, the global ICT industry remained resilient, with estimated worldwide spending reaching US$4.8 trillion in 2023. The Canadian ICT sector, in particular, is expected to generate $270 billion in revenues in 2023, marking a 5% annual growth.

Francis Bellido on why Quantum eMotion's QRNG is the ultimate weapon against cyber threats

written by InvestorNews | February 27, 2024

In a recent InvestorNews interview hosted by Brandon Colwell, Quantum eMotion Corp.'s (TSXV: QNC | OTCQB: QNCCF) President, CEO, and Director, Francis Bellido, shed light on the company's innovative Quantum Random Numbers Generator (QRNG) and its potential to revolutionize cybersecurity. Highlighting the alarming rise in cyberattacks globally, Francis discusses why the need for enhanced cybersecurity solutions has never been

more critical.

How the Quantum Encryption Approach to Cybersecurity is Virtually Unhackable

written by InvestorNews | February 27, 2024
In a recent InvestorIntel interview with Tracy Weslosky, Quantum eMotion Corp.’s (TSXV: QNC | OTCQB: QNCCF) President, CEO, and Director, Francis Bellido, shed light on the innovative approach his company is taking in the realm of cybersecurity.

The Cyber threat is real, and Cybersecurity is investible.

written by InvestorNews | February 27, 2024
Back in May of this year the world was reminded of how much of a threat cyberattacks or hacking play in our daily lives. You often hear stories about an individual or a company that suffers a ransomware attack and has to cough up gift cards or cryptocurrency as payment, or, perhaps, your personal information was stolen from someone’s database putting you at risk of identity theft and other types of fraud, all of which are bad. However, the Colonial Pipeline hack had much greater

ramifications on a large swath of the U.S. This time it wasn't the loss of information or merely the cost of the ransom (which wasn't particularly outrageous at approximately $4.4 million worth of bitcoin at the time) that was the worrying part, but the fact that a critical piece of U.S. infrastructure was basically brought to its knees by a foreign interest.

The Colonial Pipeline carries gasoline, diesel and jet fuel from Texas to as far away as New York. About 45% of all fuel consumed on the East Coast arrives via the pipeline system and life got pretty crazy, pretty quickly for over 25% of Americans. Things got so bad that President Joe Biden declared a state of emergency on May 9 followed by Georgia Governor Brian Kemp the following day. American Airlines changed flight schedules temporarily due to fuel shortages at the main airport in Charlotte, NC, while fuel shortages began to occur at gas stations amid panic buying in Alabama, Florida, Georgia, North Carolina, and South Carolina. Granted this wasn't life threatening for the most part given that the outage was relatively short lived, it, the outage, nevertheless shone a giant spotlight on the importance of cybersecurity, especially in light of what other critical infrastructures could be hacked or incapacitated.

Without digressing into whether this was ultimately state sponsored activity, or simply for profit, as the alleged hackers claimed, it exposed a weakness that is rife within both the private and the public sectors. It even exposed a threat to your personal safety and wellbeing when you think about whether the system or utility that provides your household with heat in the winter or AC in the heat of summer were to become incapacitated. I'm sure we've all seen, or at least heard of, videos of an autonomous car that gets hacked and you lose control of the gas or brake pedal. Technology has become ingrained in our day-to-day lives, likely even more so than you realize, and I'm pretty

sure we're only going to get more dependent on it in the future.

Now that I've done my best to scare the pants off everyone, what is the investment thesis here? I hope it's pretty obvious that cybersecurity is where this is headed. Despite the fact that many publicly traded cybersecurity stocks have seen pretty impressive returns over the last 12 months, I firmly believe we are still in the early innings of this trade. There are still hundreds, if not thousands, of connected entities around the world that don't have adequate protection from the threats of those with malicious intents. Granted many likely believe they are fine with what they have. In fact, I'm sure Colonial Pipeline thought they were covered. But as more and more events like this happen around the world and companies, governments and everyone else in between realizes there is value to protecting their systems, you know the revenue generation capacity of those who are good at providing cybersecurity will continue to grow.

Unfortunately, I don't know the best way to invest in this sector. As a big Formula 1 fan, I thought if the Ferrari team was willing to entrust all their data with Kaspersky then that would be good enough for me, but Kaspersky isn't currently publicly traded. So I went back to the drawing board. The largest cybersecurity ETF based on assets under management is the First Trust NASDAQ Cybersecurity ETF (NASDAQ: CIBR), which is up 55% over the last year. The fund is described as focusing on cybersecurity companies, as so classified by the Consumer Technology Association, which means CIBR holdings are primarily software and networking companies. Top holdings include Accenture (NYSE: ACN) and Cisco Systems (NASDAQ: CSCO), which aren't exactly pure play cybersecurity equities but its other holdings include Okta (NASDAQ: OKTA), Cloudflare (NYSE: NET), and Zscaler (NASDAQ: ZS). The second largest ETF, the ETFMG Prime Cyber Security ETF (NYSE ARCA: HACK), splits the industry into 2 segments: (1), developers of cybersecurity hardware or

software, and (2), providers of cybersecurity services. Here you find many of the same names in HACK as in the top 10 holdings of CIBR including Tenable Holdings (NASDAQ: TENB) and Splunk (NASDAQ: SPLK).

But if you want more of a pure play on this sector, I like either the Global X Cybersecurity ETF (NASDAQ: BUG) or iShare Cybersecurity and Tech ETF (NYSE ARCA: IHAK), both of which select holdings based on revenue, which must be at least 50% generated from cybersecurity activities. If you want to go one step further and invest in an individual equity then a look at the top holdings of these two ETFs, cross referenced with the two big ones mentioned above allows you to cull the list to Palo Alto Networks (NYSE: PANW) and CrowdStrike Holdings (NASDAQ: CRWD), which are top 10 holdings in all four of these ETFs. Its not only that all of these ETFs hold the above two mentioned equities, and likely many more. I simply focused on the funds' biggest holdings, which often drive the majority of an ETF's returns. Regardless, make sure you protect your data as best you can, because today there is always someone out to get it, which is also why everyone should be able to profit from owning at least some of these ETFs or some of the most popular of their holdings.

Biden's defense plan and some stocks set to benefit

written by InvestorNews | February 27, 2024

Yesterday marked a turning point in US history as President Joe Biden was inaugurated as the 46th President of the United

States. Much of the focus has been on Biden's policies regarding an American Rescue Plan and Biden's $2 trillion green infrastructure and jobs plan; however today I take a look at Biden's defense plan and what it means for the sector, including the defense metals companies.

Biden was a member of the Senate Foreign Relations Committee for 12 years. In that time Biden helped shape U.S. foreign policy on terrorism, weapons of mass destruction, the Middle East, Southwest Asia, and the end of apartheid. Biden favors nuclear de-escalation and has promised to renew New START, the New Strategic Arms Reduction Treaty. A key summary of what Biden will do is stated by Defense News:

"**To affordably deter Russia and China**, **Biden said he would shift investments from "legacy systems that won't be relevant" to "smart investments in technologies and innovations – including in cyber, space, unmanned systems and artificial intelligence**."

US cybersecurity

The leading cybersecurity ETF is the ETFMG Prime Cyber Security ETF (NYSE Arca: HACK). Top holdings of interest include CrowdStrike Holdings (NASDAQ: CRWD), Zscaler (NASDAQ: ZS), and FireEye (NASDAQ: FEYE).

Space

The iShares U.S. Aerospace & Defense ETF (CBOE: ITA), SPDR S&P Aerospace & Defense ETF (NYSE Arca: XAR), Procure Space ETF (NASDAQ: UFO) and the SPDR S&P Kensho Final Frontiers ETF (NYSE Arca: ROKT) are four ETFs that broadly cover aerospace and some defense stocks. Maxar Technologies (NYSE: MAXR) is a key holding in three of these ETFs. Maxar specializes in manufacturing communication, earth observation, radar, and on-orbit servicing satellites, satellite products, and related services. Some other

key aerospace and defense stocks include Northrop Grumman (NYSE: NOC), Lockheed Martin Corporation (NYSE: LMT), and Boeing (NYSE: BA).

The Procure Space ETF (UFO) summary of exposure to space related industries

Source

Unmanned systems (including unmanned aerial vehicles (UAVs))

UAVs are increasingly being used by the military for surveillance and other operations such as border patrolling, combating terrorism, and intelligence gathering ('spying'). The largest UAV companies by market share include Northrop Grumman Corporation, General Atomics Technologies Corp. (private), Boeing, Textron Inc. (NYSE: TXT) and AeroVironment Inc. (NASDAQ: AVAV). Boeing is growing in military drones/UAVs with several US Defense contracts including the Airpower Teaming System ("Loyal Wingman") military UAV. It will use artificial intelligence to fly alone or with other aircraft.

An unmanned Aerial Vehicle (UAV) patrolling the earth

Source: iStock

Artificial intelligence *(AI)*

AI stocks involved in security (facial and voice recognition etc), UAVs/drones, autonomous vehicles, space technology, and the defense sector in general stand to be the winners. Elon Musk's SpaceX and Tesla (NASDAQ: TSLA) are rapidly becoming global leaders in AI.

***Defense metals* stocks**

Generally speaking the rare earth magnet metals, uranium (for nuclear weapons etc), and key critical materials companies (cobalt for jet engines, scandium for lightweighting) have potential to do well.

Defense Metals Corp. (TSXV: DEFN | OTCQB: DFMTF) is an advanced mineral exploration company focused on metals and elements (including rare earths) commonly used in the electric vehicle (EV) market, military, national security and in green energy technologies; such as high strength alloys and rare earth magnets.

IBC Advanced Alloys Corp. (TSXV: IB | OTCQB: IAALF) makes mission-critical metal alloys and produces parts for use in U.S. defense systems, such as the F-35 jet and next-generation nuclear submarines, as well as in multiple commercial applications.

Neo Performance Materials Inc. (TSX: NEO) manufactures advanced industrial materials with a focus on magnetic powders and magnets, specialty chemicals, metals, and alloys. You can read more on them here.

Closing remarks

It is always good to have some defense stocks in your portfolio just in case we get a terrorist event or a deterioration in relations between the USA and some recent adversaries such as China, Russia, Iran, or North Korea.

Under President Biden defense spending will move towards smarter high tech methods of protecting US security. This means cybersecurity, space (satellites etc), unmanned systems (UAVs) and greater use of AI.

While global tensions are calm it may be the right time to buy into some new economy defense sector names or defense metals suppliers. What's your favorite Biden defense stock?

Apathy Let Cambridge Analytica Abuse 50 million Facebook Accounts

written by Peter Clausi | February 27, 2024

It was revealed last week that Cambridge Analytica abused personal information from 50 million Facebook accounts in early 2014 to build a system to profile individual American voters for the 2016 presidential election. The goal was to then target the users with personalised political advertisements attacking Hilary Clinton and loving The Donald. It's still not clear whether this was illegal or merely repugnant.

Most people are focussing on the fact that Cambridge Analytica was headed at the time by Steve Bannon, which provides yet another malodorous link to Trump. Facebook's share price is down about 12% but so far there has been no accountability apart from the inevitable class action litigation lawyers circling. What matters the most here is that we are becoming de-sensitized to data breaches like this.

$300M of Etherium permanently lost. Hey, it's just crypto and it wasn't mine, so who cares?

Do you know anyone who lost sleep over 143 million Americans and 100,000 Canadians that were exposed by Equifax's massive data

breach.

Every Yahoo account was compromised in 2013, which Yahoo did not figure out until 2017. That was 3 billion accounts. You likely had one of those accounts. Did you complain about it?

Citibank failed to protect the personal data (including birthdates and Social Security numbers) of approximately 146,000 customers who filed for bankruptcy between 2007 and 2011. That's adding insult to injury.

40 million Target customers were exposed in 2013. The remedial cost to Target, not including the class action litigation, was roughly $252M. Did you join the class to get your rightful piece of the settlement?

$81 million stolen from the Bank of Bangladesh by compromising the Swift system in 2016. This was the second time Swift was used as a medium of theft. But hey, that could never happen over here in the civilized world, right?

Look at the lists here and here and here for some of the largest data breaches of all time. How many of these do you remember, or care about?

Even worse, according to the Online Trust Alliance in its terrifying *Cybersecurity and Breach Trends Report* from January of this year, is that 93% of these breaches were self-inflicted and easily preventable. Apathy is our real enemy.

And next up are the assaults from Artificial Intelligence.

AI spans a broad area. A Nest WiFi-enabled thermostat can self-regulate if it feels the sun directly on it rather than air in the home environment – is that 'intelligent' or just good programming? Cruise control on your car? A video game that gets harder the further you go and that learns your favourite moves?

Neural networks? Deep learning? The hated robo-advisor? Predictive weather analysis? Smart tokens in the ICO universe?

AI is just a software operating in a hardware environment, but somehow it has gained noble status. Perhaps it's the use of the word "intelligence" that lulls us into thinking that the software is actually alive.

It's not. It's just software, a compendium of zeros and ones that open and close circuits inside chips. Software is vulnerable to coding errors, intentional or negligent. It's vulnerable to breakdowns in its hardware. And it's entirely vulnerable to malicious third parties for cryptojacking.

Our courts and insurers will have to address who becomes liable when those things go wrong. The worse situation is where software causes death, like earlier this week when a self-driving car killed a woman in Tempe, Arizona. Elaine Herzberg was walking her bicycle when she was hit by a vehicle in autonomous mode going 40 km/h. It doesn't take a crystal ball to see Mr. Herzberg is the first of many such deaths.

Who will carry the financial burden of the error when smart tokens co-ordinate a contract for one billion rolls of toilet paper when the intention was for 100 rolls of paper towel? Is this contract law or negligence? Can you contract out of liability? Medical diagnostic software misses an obvious cause resulting in patient death? Who pays the repair bills when Skynet finally goes live and the Terminator kicks in your door?

Vernor Vinge's 1993 short paper *The Coming Tehnological Singularity* is a marvel of literature that manages to inspire and terrify at the same time. Should something we created actually develop its own intelligence, the pace at which technology would from that point develop would be inconceivable to humans. The human era would be over.

Back to the breaches, both malicious and self-inflicted. Incompetence and thievery have been with humanity for recorded history. The first trojan horse was the serpent surreptitiously attacking the Old Testament God by way of his human creations and an apple. Sadly, we do need various levels of government to help us defend ourselves. This will require some levels of regulation, even if unwanted.

The CryptoCrowd may not like it, but regulation is needed and it's coming. At least there seems to be some regulatory recognition that data is a different world requiring a different set of regulatory parameters. See for example the British Columbia Securities Commission's 2018 outreach efforts seeking innovation while maintaining confidence in the capital markets.

This apathy is a strange mindset, especially since the business world otherwise takes confidentiality seriously. We sign confidentiality agreements and NDA's. We expect our employees to leave our IP at the office. Securities laws exist to prevent insider trading and to protect the dignity of the market. Larger boards have committees specializing in privacy and data protection. There are few things more valuable to any company than the integrity of its data.

So we should be outraged by these ongoing assaults on us, our data and our companies. We should be in the streets, with torches and pitchforks, demanding that heads roll and attackers be found. Instead, we shrug and say "What can we do? I'm just one helpless person. The government will protect us." That only goes so far.

We have to use what the government gives us. CASL (Canada's AntiSpam Legislation) is a horribly mis-named piece of legislation that has teeth. It codifies an individual's right to control the inbox. It isn't about spam, it's about your digital

liberty.

The GDPR is the European Union’s approach, and it’s a good one. A prior article explaining GDPR is here. Recent recommendations from House of Commons Standing Committee on Access to Information, Privacy and Ethics indicate that Canada will adopt an approach similar to GDPR to give you the tools to protect yourself. So use them.

Ultimately, it’s up to you. Be vigilant. Protect your local network. Follow good protocols. Don’t be sloppy. And be angry over every breach. Demand accountability. Next time it could be you.