

# EQUITY RESEARCH

March 6, 2022

ESG

## The Increased Risk Of Cyber Crimes

Russia-Ukraine Conflict Brings Cyber Security Into Focus

### Our Conclusion

The longer-term implications of the Russia-Ukraine conflict largely remain unknown, but it is reasonable to assume an elevated cyber risk in the future. Cyber attacks are possible at any time, but in an environment of heightened tensions in Europe, we advise issuers and investors to have a cyber incident response plan in place.

For investors looking to gain exposure to cyber security, we specifically highlight the Nasdaq First Trust Cybersecurity ETF (CIBR US) and the Evolve Cyber Security Index Fund (CYBR CN) as the largest ETFs in the U.S. and Canada, respectively. For investors looking for specific Canadian equities, we also reference CGI and Magnet Forensics as having leading cyber security service offerings.

### Key Points

The risk of cybercrime has been increasing each year. Globally, there is a cyber attack at least every 49 seconds. Last year's most notable cyber-attack was on the Colonial Pipeline system, which affected almost half of the U.S. East Coast fuel supply. For those interested, testimony of that day's events to Congress can be viewed [here](#).

Cyber risk is still an emerging threat, and it is important for business to stay ahead of the curve as much as possible. For those looking to get up to speed on the topic, we provide a comprehensive list of questions to assist investors in gauging management's level of preparedness of a cyber event. This list can be seen in Appendix 1 on page 7 of this report.

From an ESG perspective, carbon emissions tend to get the most attention. Governance issues tend to be the least mentioned across ESG. However, we have seen increased awareness of governance topics – most recently around dual-class share structures and insider ownership. We believe the importance of data protection will also continue to increase over time and become a key governance topic.

At a time when global supply chains are already stressed, it is important for investors and businesses to also think of the cyber risk across the supply chain. If the regrettable situation in Ukraine has taught us anything, political risk and general concerns about the security of (commodity) supply chains are back in focus. This has read-throughs to the security of data across supply chains as well.

**Shaz Merwat**  
+1 416-956-6428  
Shaz.Merwat@cibc.com

**Jin Yan, CFA**  
+1 416-594-8877  
Jin.Yan@cibc.com

**Ian de Verteuil**  
+1 416-594-7462  
Ian.deVerteuil@cibc.com

**Katsiaryna Kulbitskaya**  
+1 416-956-6223  
Katsiaryna.Kulbitskaya@cibc.com

**Jinzhu Zhai**  
+1 416-581-2164  
Jinzhu.Zhai@cibc.com

### Sectors:

Portfolio Strategy, ETF Research



Environmental



Social



Governance



## The Ukraine Conflict Risks A Spike In Cyber Crime

Almost two weeks into the Ukraine conflict and we still lack clarity into an expected outcome. Over the last week, it appears Western sanctions are having an impact on the Russian economy; the central bank hiked interest rates to 20%, cash exports of foreign currency are limited to US\$10,000 and the country's stock exchange has remained closed since February 28.

Russia is a leading state-sponsor of cyber crime

How the situation unfolds remains uncertain, but it seems Putin is intent on increasing Russia's sphere of influence on the continent. Economically, the country is the 11<sup>th</sup> largest in the world (13<sup>th</sup> assuming a 10% GDP decline this year), but militarily it is a world leader. The country is also one of the most sophisticated state-sponsors of cyber activity. The bar charts in Exhibit 1 show the most active state-sponsors of cyber activity (proxied here by types of ransomware), with all the usual suspects. Iran and Russia top the list.

### Exhibit 1: State-sponsored Cyber Activity – Ransomware Strains By Country, Current

Ransomware strains linked to specific countries



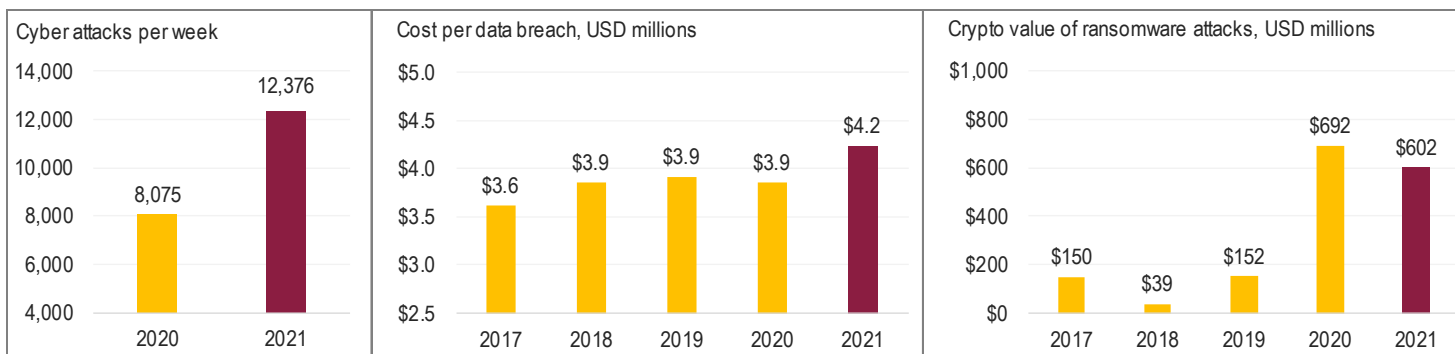
Source: Chainalysis and CIBC World Markets Inc.

The largest cyber-attacks in the last two years were linked back to Russia; first, the SolarWinds hack in 2020 affecting thousands of organizations across U.S. public and private sectors, and the Colonial Pipeline ransomware attack in May of last year. The latter led to Colonial shutting down its pipeline system for days, affecting almost half of the U.S. East Coast fuel supply and leading to gasoline price spikes and shortages.

On average, a cyber-attack occurs every 49 seconds

Even before the Ukrainian situation, cyber-attacks have been on the rise. As the bar charts show in Exhibit 2, cyber attacks were up 50% in 2021 (left chart) and the average cost of a data breach rose to US\$4.2 million (middle chart). The total crypto dollar value of ransomware attacks (where hackers hijack information or IT systems and then demand a ransom) accounted for about US\$600 million (right chart). Almost three-quarters of this US\$600 million in 2021 was traced back to Russian hackers.

### Exhibit 2: Cyber Risk – Number Of Cyber Attacks, Cost Per Data Breach And Ransomware Cost – Last Five Years



Source: Check Point, IBM, Chainalysis and CIBC World Markets Inc.

It is reasonable to expect the level of cyber activity to increase in the future. Even if peace comes to Ukraine in the near term, the global isolation around Russia is likely to stay in place for years, given the events that have already transpired. Companies from countries placing sanctions on Russia are also likely at elevated levels of cyber risk.

## Cyber Security In The Context Of ESG

In the world of ESG, the “G” (governance) gets little attention. This is largely the case for two reasons. Firstly, there has been an overwhelming focus within ESG on environmental (greenhouse gas) concerns. Secondly, the consideration of governance issues is already widely adopted in traditional investment analysis.

Data protection is often an overlooked ESG topic, but becoming more important

Typical governance metrics such as executive compensation, insider ownership, dual-class share structures are all important, but over the last few years cyber security has increasingly become a key governance concern. This makes sense given the wide adoption of technology and businesses’ reliance on information/data systems in everyday business operations.

Data protection in the context of ESG is seen as most relevant to sectors where services are either internet-based such as Information Technology and Communication Services (e-commerce, cloud-based services, etc.), or those involving sensitive digital information such as Financials and Health Care (account details, medical records, etc.).

SASB’s disclosure standards for these sectors include data protection-related metrics. This includes disclosing the number of data breaches, the percent of breaches involving personally identifiable information, and a description of the approach to identify data security risks, to name a few. For more detail, please see SASB’s Materiality Finder (see [link](#)).

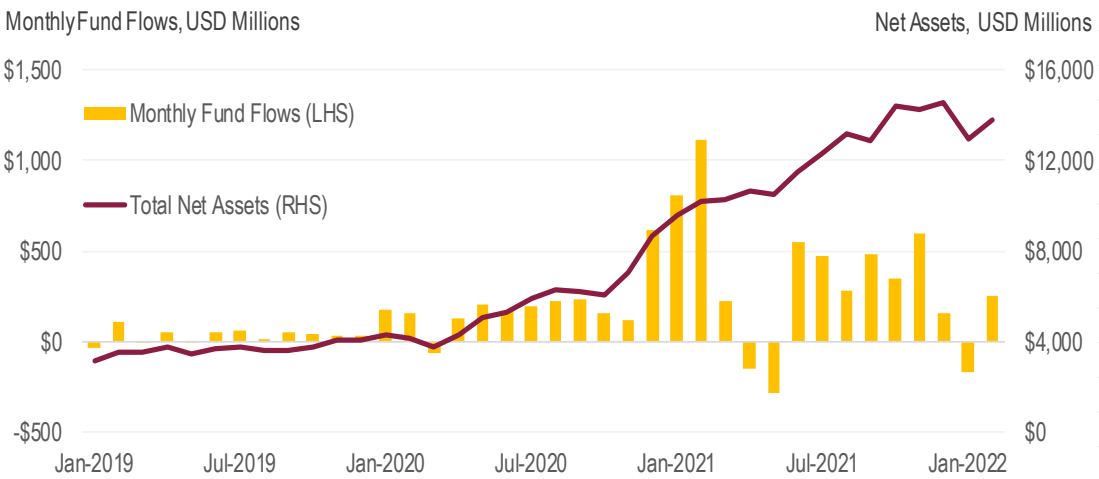
19 questions to help investors gauge the level of cyber preparedness

Having said this, businesses across all sectors are vulnerable to cyber risk. For investors looking to get up to speed on the topic, we present a list of questions in Appendix 1 that is a good starting point when engaging with management in assessing the level of preparedness for a cyber event.

## Investment Opportunities Arising from Cyber Risk

One of the easiest ways to gain financial exposure to this topic is to invest in businesses providing data protection services via a cyber security ETF. Since the start of 2019, cyber security ETFs have consistently seen net inflows and have gathered US\$7.4B of new assets. Coupled with strong performance of the underlying equities, this has resulted in total assets held within cyber security ETFs reaching about US\$14B currently. This can be seen in the bar/line graph shown below in Exhibit 3.

Exhibit 3: Cyber Security ETFs – Monthly Fund Flows And Net Assets, Jan. 2019 To Date



Source: Bloomberg and CIBC World Markets Inc.

In the table in Exhibit 4, we include a list of the largest cyber security ETFs globally. The First Trust NASDAQ Cybersecurity ETF (CIBR US) is the largest and most actively traded cyber security ETF. The ETF tracks the Nasdaq CTA Cybersecurity Index, whose constituents are determined by the Consumer Technology Association. The Canadian-listed CIBR CN is essentially a wrapper for the larger U.S.-listed ETF.

CIBR US and CYBR CN are the largest cyber security ETFs in the U.S. and Canada, respectively

Evolve's CYBR is the largest cyber security ETF in Canada. The ETF tracks the Solactive Global Cyber Security Index, which consists of a mix of Software & Services and Equipment companies. The ETF is offered in multiple currency options, including CAD-Hedged (CYBR CN), CAD-Unhedged (CYBR/B CN), and USD (CYBR/U CN).

The recently launched Horizons GX Cybersecurity Index ETF (HBUG CN) is essentially a wrapper for the larger Global X Cybersecurity ETF (BUG US), with the added feature of FX hedging. In comparison with other cyber security ETFs, HBUG's exposure to Software & Services companies is the highest at 90%+ of the portfolio.

For additional trading statistics around these ETFs, refer to the table in Appendix 2.

#### Exhibit 4: Cyber Security ETFs – Largest ETFs By Fund AUM, North America And International, Current

Ticker	ETF Name	AUM USD mln	MER	Underlying Index
<b>North America-Listed</b>				
CIBR US Equity	First Trust NASDAQ Cybersecurity ETF	5,944	0.60	Nasdaq CTA Cybersecurity Index
HACK US Equity	ETFMG Prime Cyber Security ETF	2,049	0.60	Prime Cyber Defense Index
BUG US Equity	Global X Cybersecurity ETF	1,166	0.50	Indxx Cybersecurity Index
IHAK US Equity	iShares Cybersecurity and Tech ETF	587	0.47	NYSE FactSet Global Cyber Security Index
CYBR CN Equity	Evolve Cyber Security Index Fund	196	0.63	Solactive Global Cyber Security Index
WCBR US Equity	WisdomTree Cybersecurity Fund	40	0.45	WisdomTree Team8 Cybersecurity Index
CIBR CN Equity	First Trust Nasdaq Cybersecurity ETF	28	0.76	Nasdaq CTA Cybersecurity Index
HBUG CN Equity	Horizons GX Cybersecurity Index ETF	2	0.55 *	Indxx Cybersecurity Index
<b>Internationally-Listed</b>				
USPY LN Equity	L&G Cyber Security UCITS ETF	2,858	0.69	ISE Cyber Security UCITS Index
HACK AU Equity	BetaShares Global Cybersecurity ETF	550	0.67	Nasdaq CTA Cybersecurity Index
CIBR LN Equity	First Trust Nasdaq Cybersecurity UCITS ETF	373	0.60	Nasdaq CTA Cybersecurity Index
CYBR LN Equity	Rize Cybersecurity and Data Privacy UCITS	133	0.45	Foxberry Tematica Research Cybersecurity & Data Privacy Index
HRLF204 IT Equity	Harel Sal 4A ISE Cyber Security Dollar-Hedged	124	0.63	ISE Cyber Security Index
WCBR LN Equity	WisdomTree Cybersecurity UCITS ETF	67	0.45	WisdomTree Team8 Cybersecurity Index
00875 TT Equity	Cathay Cyber Security ETF	42	1.18	ISE Cyber Security Index

Note: \*MER is estimated as the actual MER is not yet available. Source: Bloomberg and CIBC World Markets Inc.

Although the ETFs in the above list each provide similar exposure and have significant overlaps, there are some differences in their underlying methodologies. This can result in differences in holdings. In the table in Exhibit 5, we provide a summary of some of the most widely tracked cyber security indices and their respective methodologies.

**Exhibit 5: Cyber Security Indices – Index Methodologies, March 2022**

	Nasdaq CTA Cybersecurity Index	Indxx Cybersecurity Index	Solactive Global Cyber Security Index	NYSE FactSet Global Cyber Security Index
<b>ETFs</b>	CIBR US CIBR CN (CAD-Unhedged) CIBR LN HACK AU	BUG US HBUG CN (CAD-Hedged)	CYBR CN (CAD-Hedged) CYBR/B CN (CAD-Unhedged) CYBR/U CN (USD)	IHAK US XHAK CN (Listing-pending)
<b>Universe</b>	<ul style="list-style-type: none"> <li>Global Nasdaq Eligible Exchanges</li> <li>Min market cap US\$250mm</li> <li>Min 3-mth ADV US\$1mm</li> <li>Min free float 20%</li> </ul>	<ul style="list-style-type: none"> <li>Global equities (Developed + Emerging markets)</li> <li>Min market cap US\$200mm</li> <li>Min 6-mth ADV US\$2mm</li> <li>Traded on 90% of trading days in last 6 months</li> <li>Min free float market cap of \$1B</li> </ul>	<ul style="list-style-type: none"> <li>Global Developed markets</li> <li>Min market cap of CAD\$100mm</li> <li>Min 3-mth ADV of CAD\$2mm</li> </ul>	<ul style="list-style-type: none"> <li>Global equities (Developed + Emerging Markets)</li> <li>Min market cap of US\$300mm</li> <li>Min 3-mth ADV of US\$2mm</li> </ul>
<b>Index Criteria</b>	Companies classified as a Cybersecurity company by Consumer Technology Association	Companies in various Software Services and Communications industries (as determined by FactSet) that derive 50%+ of their revenues from cybersecurity activities	Companies in these FactSet RBICS sub-industries: <ul style="list-style-type: none"> <li>Carrier Edge Network Management Equipment</li> <li>Customer Premises Network Security Equipment</li> <li>Co-location and Data Center Services</li> <li>Government IT Services</li> <li>Network Security Access Policy Software</li> <li>Network Security Software</li> </ul>	Companies that derive 50%+ of their revenues from Cyber Security-related FactSet RBICS industries, including Hardware and Software Services
<b>Rebalance Schedule</b>	Reconstituted semi-annually in March and September; rebalanced quarterly in March, June, September, and December	Semi-annually in May and November	Quarterly in January, April, July and October	Reconstituted annually in December; rebalanced semi-annually in June and December
<b>Weighting</b>	Liquidity-weighted, with a security weight cap of 6%	Cap-weighted, with a security weight cap/floor of 6% / 0.3%	Cap-weighted, with a security weight cap of 7.5%	Cap-weighted, with a security weight cap of 4%
<b>Constituents</b>	35	31	57	54

Source: Index methodology documents and CIBC World Markets Inc.

Blackberry is the most held Canadian equity within the cyber ETF universe

From a constituent perspective, the largest-held cyber security equities in this ETF universe are Palo Alto Networks, Cisco Systems and Check Point Software. A list of the ten most widely held equities held is shown in the Exhibit 6 table, which account for about one-third of the total universe. The most held Canadian equity in this universe is Blackberry, ranked 33<sup>rd</sup> globally.

**Exhibit 6: Cybersecurity ETFs – List Of Top Equities Held Globally, Current**

Rank	Name	USD Millions	% of Universe	Rank	Name	USD Millions	% of Universe
1	Palo Alto Networks Inc	708	5.1%	6	Mandiant Inc	456	3.3%
2	CISCO Systems Inc	571	4.1%	7	Trend Micro Inc	408	2.9%
3	Check Point Software Tech	571	4.1%	8	Juniper Networks Inc	402	2.9%
4	CrowdStrike Holdings	558	4.0%	9	CyberArk Software Ltd	392	2.8%
5	Fortinet Inc	458	3.3%	10	Splunk Inc	372	2.7%
<b>Top 5 Largest Holdings Total</b>		<b>2,866</b>	<b>20%</b>	<b>Top 10 Largest Holdings Total</b>		<b>4,896</b>	<b>35%</b>

Source: Bloomberg and CIBC World Markets Inc.

Magnet Forensics and CGI  
are two of Canada's leading  
cyber security providers

Within CIBC's Canadian Technology coverage, we highlight Magnet Forensics and CGI as best positioned from an increased demand for cyber security services. Magnet Forensics is a leading provider of digital investigation tools for public safety and corporate clients. The company has recently extended its law enforcement digital forensics solutions into the corporate market, including tools to assist with incident response and investigations in cyber security incidents.

CGI is a more complete cyber security provider, with a dedicated cyber security practice of 1,700 security specialists, and service offerings covering a wide spectrum of cyber security. This includes advisory services, security engineering, and managed security services. We would also note as the frequency and magnitude of corporate cyber security breaches increases, demand for post-incident investigations is also likely to grow.

## Appendix 1: Cybersecurity Questions For Investors

### Exhibit 7: Management Questions – Possible Cybersecurity Questions For Investors To Ask Management

Questions For Management	How To Gauge Management's Response
Who is responsible for cyber security?	The CEO should be responsible for driving security governance, investment and planning, but day-to-day responsibilities are often delegated. Each employee has a part to play.
Do you have a current cyber incident response plan? Can we see it?	The plan should detail who is responsible in managing a breach, who else is involved in the process (Communications, Legal, IT specialists, etc.) and how current is the plan.
Can someone in the organization brief me on your cyber risk profile?	In essence, it matters more whether the company can articulate responsibility, which should provide information as to how rigorously they've thought of their cyber security management.
How many attacks were seen last quarter/month/week?	The key to a good response here is simply having awareness to the current status.
What have you learned from previous cyber incidents?	Incidents should be treated as opportunities to learn and bridge the gap. Zero reported threats could easily mean breaches are yet to be identified.
Have any independent tests been done?	With increasing regulation, it will be paramount for companies to demonstrate their fiduciary duty towards stakeholders with a responsible risk mitigation process in place. Third-party verification would limit any possible legal/regulatory ramifications from a future breach.
Is cyber-security classified as one of your corporate risks?	IT risks can often be arcane to the average employee, but the translation of the technical nature of the risk needs to transcend to the senior management and the board of directors.
How much would it cost if you lost all your IT systems for a day?	This is meant to gauge whether senior management has a true understanding of the cost of an IT interruption to operations, which is often underestimated.
What is the most valued information at this firm?	Ideally, the company has a more robust data protection system in place around the company's "crown jewels." It also shows management understands where the most impactful breaches are likely to occur.
What is the annual cyber security budget?	Typically, this amounts to about 5% to 10% of an IT budget.
How is cyber security risk disclosed?	This allows investors to keep up to date with how management is adapting to the nature of cyber security.
Is there business interruption insurance in place to deal with a cyber breach?	Understanding whether the company is covered in case of a cyber breach will help investors evaluate the potential fallout from a possible incident.
Do you have communication obligations to clients, employees, investors, regulators, etc. in a investment community and regulators in case of an incident. This should help reduce volatility and cyber breach? Is there legal advice to guide you?	Understanding roles and responsibilities should allow for clear and concise messaging to customers, the clients, employees, investors, regulators, etc. in a investment community and regulators in case of an incident. This should help reduce volatility and cyber breach? speculation on share price should an event ever occur.
Do you have a back-up site in place?	Effectively, what is Plan B?
Are employees well-versed as to how to deal with a cyberattack?	This question should help provide color as to how well the risk is understood across the organization. If an employee's system is overtaken by malware, does he/she know what to do?
Is there a call-tree/contact list in place?	Should be easily accessible so as not to waste time in bureaucracy in case of an actual cyber event.
Has the firm undertaken fire drills to test the response plan?	Practice makes perfect, and routine mock exercises should be run to test operational procedures.
Does the company participate in industry forums?	Hacktivists are extremely sophisticated and often state-sponsored. Shared learning and best practices are a way to stay ahead of the curve.
What are the top five cyber risks you face today?	The ability to specifically pinpoint risks should provide reassurance the company has spent the time to think this through. It also can gauge how the company sees the risks evolving over time.

Source: CIBC World Markets Inc.



## Appendix 2: Notable Cyber Security ETFs Trading Statistics

Exhibit 8: Cyber Security ETFs – Notable Cyber Security ETF Trading Statistics, Current

Ticker	Total NAV Return (Local Currency)					NAV Return Volatility		Avg Spread
	4wk	YTD	1yr	3yr	5yr	3mth	1yr	20day
<b>North America-Listed</b>								
CIBR US Equity	6.92	-3.24	19.7	85.31	149.23	30.4	20.59	0.09%
HACK US Equity	5.79	-5.23	2.51	48.17	107.46	27.28	19.54	0.21%
BUG US Equity	10.3	-0.98	18.32	na	na	33.69	25.31	0.23%
IHAK US Equity	4.39	-5.29	6.84	na	na	30.71	20.94	0.14%
CYBR CN Equity	7.22	-5.96	0.5	69.15	na	38.71	25.62	0.47%
WCBR US Equity	7.13	-7.83	6.28	na	na	43.77	30.41	0.50%
CIBR CN Equity	6.81	-3.51	19.43	na	na	32.28	19.77	0.14%
HBUG CN Equity	10.66	-0.36	na	na	na	na	na	0.38%
<b>Internationally-Listed</b>								
USPY LN Equity	3.66	-6.48	0.31	51.69	128.08	28.36	19.47	0.33%
HACK AU Equity	3.47	-4.45	26.71	77.22	153.69	33.35	18.26	0.24%
CIBR LN Equity	6.86	-3.3	19.44	na	na	30.06	20.61	0.48%
CYBR LN Equity	2.72	-9.29	-1.45	na	na	29.05	22.11	0.54%
HRLF204 IT Equity	2.8	-8.94	na	34.73	na	27.11	22.04	0.69%
WCBR LN Equity	7.12	-7.85	6.16	na	na	44.37	30.42	0.57%
00875 TT Equity	8.23	-6.71	-3.38	na	na	25.42	19.25	0.18%

Source: Bloomberg and CIBC World Markets Inc.



## Important Disclosures

**Analyst Certification:** Each CIBC World Markets Inc. research analyst named on the front page of this research report, or at the beginning of any subsection hereof, hereby certifies that (i) the recommendations and opinions expressed herein accurately reflect such research analyst's personal views about the company and securities that are the subject of this report and all other companies and securities mentioned in this report that are covered by such research analyst and (ii) no part of the research analyst's compensation was, is, or will be, directly or indirectly, related to the specific recommendations or views expressed by such research analyst in this report.

**Potential Conflicts of Interest:** Equity research analysts employed by CIBC World Markets Inc. are compensated from revenues generated by various CIBC World Markets Inc. businesses, including the CIBC World Markets Investment Banking Department. Research analysts do not receive compensation based upon revenues from specific investment banking transactions. CIBC World Markets Inc. generally prohibits any research analyst and any member of his or her household from executing trades in the securities of a company that such research analyst covers. Additionally, CIBC World Markets Inc. generally prohibits any research analyst from serving as an officer, director or advisory board member of a company that such analyst covers.

In addition to 1% ownership positions in covered companies that are required to be specifically disclosed in this report, CIBC World Markets Inc. may have a long position of less than 1% or a short position or deal as principal in the securities discussed herein, related securities or in options, futures or other derivative instruments based thereon.

Recipients of this report are advised that any or all of the foregoing arrangements, as well as more specific disclosures set forth below, may at times give rise to potential conflicts of interest.

CIBC World Markets Inc. does and seeks to do business with companies covered in its research reports. As a result, investors should be aware that CIBC World Markets Inc. may have a conflict of interest that could affect the objectivity of this report. Investors should consider this report as only a single factor in making their investment decision.

Analysts employed outside the U.S. are not registered as research analysts with FINRA. These analysts may not be associated persons of CIBC World Markets Corp. and therefore may not be subject to FINRA Rule 2241 restrictions on communications with a subject company, public appearances and trading securities held by a research analyst account.

## CIBC World Markets Inc. Stock Rating System

Stock Ratings	Abbreviation	Description
Outperformer	OP	Stock is expected to outperform similar stocks in the coverage universe during the next 12-18 months.
Neutral	NT	Stock is expected to perform in line with similar stocks in the coverage universe during the next 12-18 months.
Underperformer	UN	Stock is expected to underperform similar stocks in the coverage universe during the next 12-18 months.
Tender	TR	Shareholders are advised to tender shares to a specific offer as we do not believe a superior offer will materialize.
Not Rated	NR	CIBC World Markets does not maintain an investment recommendation on the stock.
Restricted	R	CIBC World Markets is restricted (due to potential conflict of interest) from rating the stock.

Sector Ratings	Abbreviation	Description
Overweight	O	Sector is expected to outperform the broader market averages.
Marketweight	M	Sector is expected to equal the performance of the broader market averages.
Underweight	U	Sector is expected to underperform the broader market averages.
None	NA	Sector rating is not applicable.

Note: Broader market averages refer to S&P 500 in the U.S. and S&P/TSX Composite in Canada.

## CIBC World Markets Inc. Price Chart

For price and performance charts, please visit CIBC on the web at <https://researchcentral.cibccm.com/#/disclaimer-central-new> or write to CIBC World Markets Inc., 161 Bay Street, 4th Floor, Toronto, ON M5H 2S8, Attn: Research Disclosure Chart Request.

## Important Disclosure Footnotes

For important disclosure footnotes for companies mentioned in this report that are covered by CIBC World Markets Inc., click here: [CIBC Disclaimers & Disclosures](#)

Companies mentioned in the report but not listed are not covered by fundamental research at CIBC.

Ratings Distribution\*: CIBC World Markets Inc. Coverage Universe

(as of 06 Mar 2022)	Count	Percent	Inv. Banking Relationships	Count	Percent
Outperformer	181	59.7%	Outperformer	180	99.4%
Neutral	114	37.6%	Neutral	112	98.2%
Underperformer	8	2.6%	Underperformer	8	100.0%
Tender	0	0.0%	Tender	0	0.0%
Restricted	5	1.7%	Restricted	5	100.0%

Important disclosures for each issuer can be found by visiting the Research Central website at <https://researchcentral.cibccm.com/#/disclaimer-central-new> and then entering the issuer name. Access to our research dissemination policy can be found on the same website at <https://researchcentral.cibccm.com/#/dissemination-policy>. These important disclosures can also be obtained by writing to CIBC World Markets Inc., 161 Bay Street, 4th Floor, Toronto, ON M5H 2S8, Attention: Research Disclosures Request.

## Access to CIBC Equity Research

Clients may access CIBC Equity Research online at Research Central at <https://researchcentral.cibccm.com/>, or at the following research aggregators: Bloomberg, Refinitiv, Capital IQ, and FactSet.

## Legal Disclaimer

This report is issued and approved for distribution by (a) in Canada, CIBC World Markets Inc., a member of the Investment Industry Regulatory Organization of Canada ("IIROC"), the Toronto Stock Exchange, the TSX Venture Exchange and a Member of the Canadian Investor Protection Fund, (b) in the United Kingdom, CIBC World Markets plc, is Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority, (c) in Australia to wholesale clients only, CIBC Australia Ltd, a company regulated by the ASIC with AFSL license number 240603 and ACN 000 067 256, and (d) in Japan, CIBC World Markets (Japan) Inc., a registered Type 1 Financial product provider with the registration number Director General of Kanto Finance Bureau #218 (collectively, "CIBC World Markets") and (e) in the United States either by (i) CIBC World Markets Inc. for distribution only to U.S. Major Institutional Investors ("MII") (as such term is defined in SEC Rule 15a-6) or (ii) CIBC World Markets Corp., a member of the Financial Industry Regulatory Authority ("FINRA"). U.S. MIIs receiving this report from CIBC World Markets Inc. (the Canadian broker-dealer) are required to effect transactions (other than negotiating their terms) in securities discussed in the report through CIBC World Markets Corp. (the U.S. broker-dealer). CIBC World Markets Corp. accepts responsibility for the content of this research report.

This report is provided, for informational purposes only, to institutional investor and retail clients of CIBC World Markets in Canada, and does not constitute an offer or solicitation to buy or sell any securities discussed herein in any jurisdiction where such offer or solicitation would be prohibited. This document and any of the products and information contained herein are not intended for the use of Retail investors in the United Kingdom. Such investors will not be able to enter into agreements or purchase products mentioned herein from CIBC World Markets plc. The comments and views expressed in this document are meant for the general interests of wholesale clients of CIBC Australia Ltd.

This report has been prepared by the CIBC group and is issued in Hong Kong by Canadian Imperial Bank of Commerce, Hong Kong Branch, a registered institution under the Securities and Futures Ordinance, Cap 571 (the "SFO"). This report is intended for "professional investors" only (within the meaning of the SFO) and has been prepared for general circulation and does not take into account the objectives, financial situation or needs of any recipient. Any recipient in Hong Kong who has any questions or requires further information on any matter arising from or relating to this report should contact Canadian Imperial Bank of Commerce, Hong Kong Branch at Suite 3602, Cheung Kong Centre, 2 Queen's Road Central, Hong Kong (telephone number: +852 2841 6111). Orders for Hong Kong listed securities will be executed by Canadian Imperial Bank of Commerce, Hong Kong Branch. Canadian Imperial Bank of Commerce, Hong Kong Branch has entered into an arrangement with its broker-dealer affiliates worldwide to execute orders for securities listed outside of Hong Kong for Hong Kong clients.

This report is intended for distribution in Singapore solely to "institutional investors" (within the meanings of the Financial Advisers Act (Chapter 110 of Singapore)).

The securities mentioned in this report may not be suitable for all types of investors. This report does not take into account the investment objectives, financial situation or specific needs of any particular client of CIBC World Markets. Recipients should consider this report as only a single factor in making an investment decision and should not rely solely on investment recommendations contained herein, if any, as a substitution for the exercise of independent judgment of the merits and risks of investments. The analyst writing the report is not a person or company with actual, implied or apparent authority to act on behalf of any issuer mentioned in the report. Before making an investment decision with respect to any security recommended in this report, the recipient should consider whether such recommendation is appropriate given the recipient's particular investment needs, objectives and financial circumstances. CIBC World Markets suggests that, prior to acting on any of the recommendations herein, Canadian retail clients of CIBC World Markets contact one of our client advisers in your jurisdiction to discuss your particular circumstances. Non-client recipients of this report who are not institutional investor clients of CIBC World Markets should consult with an independent financial advisor prior to making any investment decision based on this report or for any necessary explanation of its contents. CIBC World Markets will not treat non-client recipients as its clients solely by virtue of their receiving this report.

## Legal Disclaimer (Continued)

Past performance is not a guarantee of future results, and no representation or warranty, express or implied, is made regarding future performance of any security mentioned in this report. The price of the securities mentioned in this report and the income they produce may fluctuate and / or be adversely affected by exchange rates, and investors may realize losses on investments in such securities, including the loss of investment principal. CIBC World Markets accepts no liability for any loss arising from the use of information contained in this report, except to the extent that liability may arise under specific statutes or regulations applicable to CIBC World Markets.

Information, opinions and statistical data contained in this report were obtained or derived from sources believed to be reliable, but CIBC World Markets does not represent that any such information, opinion or statistical data is accurate or complete (with the exception of information contained in the Important Disclosures section of this report provided by CIBC World Markets or individual research analysts), and they should not be relied upon as such. All estimates, opinions and recommendations expressed herein constitute judgments as of the date of this report and are subject to change without notice.

Nothing in this report constitutes legal, accounting or tax advice. Since the levels and bases of taxation can change, any reference in this report to the impact of taxation should not be construed as offering tax advice on the tax consequences of investments. As with any investment having potential tax implications, clients should consult with their own independent tax adviser.

This report may provide addresses of, or contain hyperlinks to, Internet web sites. CIBC World Markets has not reviewed the linked Internet web site of any third party and takes no responsibility for the contents thereof. Each such address or hyperlink is provided solely for the recipient's convenience and information, and the content of linked third party web sites is not in any way incorporated into this document. Recipients who choose to access such third-party web sites or follow such hyperlinks do so at their own risk.

Although each company issuing this report is a wholly owned subsidiary of Canadian Imperial Bank of Commerce ("CIBC"), each is solely responsible for its contractual obligations and commitments, and any securities products offered or recommended to or purchased or sold in any client accounts (i) will not be insured by the Federal Deposit Insurance Corporation ("FDIC"), the Canada Deposit Insurance Corporation or other similar deposit insurance, (ii) will not be deposits or other obligations of CIBC, (iii) will not be endorsed or guaranteed by CIBC, and (iv) will be subject to investment risks, including possible loss of the principal invested. The CIBC trademark is used under license.

© 2022 CIBC World Markets Inc. and CIBC World Markets Corp. All rights reserved. Unauthorized use, distribution, duplication or disclosure without the prior written permission of CIBC World Markets is prohibited by law and may result in prosecution.