TSX CYBR

SPECIAL COMMENTARY

# Evolve Cyber Security Index Fund

CYBR invests primarily in equity securities of companies located domestically or internationally that are involved in the cyber security industry through hardware and software development.

As at March 17, 2020

**ETF TICKER:** CYBR (Hedged); CYBR.B (Unhedged); CYBR.U (USD)
**MUTUAL FUND FUNDSERV CODE:** EVF150 (Class F); EVF151 (Class A)

## UPDATE:

Equity indices worldwide have fallen nearly 30% since the peak of the markets on February 19th, during this period CYBR has performed in line with major equity indices, with the hedged class (CYBR) down -30.8%, and unhedged class (CYBR.B) down -26.2%.

Often, CYBR has been compared to the Nasdaq 100 Index as a reference. On a year-to-date basis, CYBR has slightly underperformed the Nasdaq 100 index, however, with much less volatility.

Since the start of the year 2020, Nasdaq 100 Index has had an annualized volatility of 54%, whereas CYBR has had an annualized volatility of 42%, translating to a better risk adjusted performance for CYBR.

Recently, the National Cyber Security Centre published advice to businesses warning them of an increased cybersecurity threat from people working from home using their personal devices.

## MACROECONOMIC HIGHLIGHTS:

Cybercrime profits reached at least US$3.5 billion in 2019, reports the FBI's Internet Crime Complaint Centre (IC3). This total is based on the 467,361 complaints from individuals and businesses received by IC3 during 2019. The actual dollar value is likely much higher, since many cybercrimes go unreported by the victims. Phishing and extortion remain the most popular ways of scamming people, with techniques becoming increasingly sophisticated, making it hard for people to tell what is legitimate and what is not. Ransomware netted criminals more than $8.9m in 2019.[i]

A novel way of using and concealing stolen credit card data has been uncovered by the U.S. Secret Service. The technique involves embedding stolen card information in barcodes affixed to phony money network rewards cards. The scammers pay for merchandise by instructing a cashier to scan the barcode and enter the expiration date and card security code. The tactic was first uncovered with cards used by Sam's Club and WalMart stores, but the Secret Service also believes scheme could be used with barcodes are stored in smartphones. This evolution of the traditional card-not-present fraud seems to have links to Asian organized crime.[ii]



Evolve ETFs
Brookfield Place, 161 Bay Street, Suite 2700, Toronto ON M5J 2S1
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com

The government of Puerto Rico has fallen victim to a Business Email Compromise (BEC) scam to the tune of US$2.6 million. Puerto Rico's Industrial Development Company mistakenly transferred the money into a bank account run by scammers after receiving an email requesting a change to the bank account tied to remittance payments. When the breach was discovered some time later the FBI was immediately informed, but it's unclear whether the Puerto Rico government will be able to recover the stolen money.[iii] According to the FBI, half of all reported cybercrime losses in 2019 came from BEC attacks.[iv]

Personal details—including full names, home addresses, phone numbers, and emails—of more than 10.6 million former guests of MGM Resorts hotels, including Justin Bieber and Twitter's chief executive, Jack Dorsey, were posted on an online hacking forum in February.

An MGM spokesperson said the information comes from a security incident in 2019 in which MGM "discovered unauthorized access to a cloud server that contained a limited amount of information for certain previous guests of MGM Resorts." The data reportedly contains no information from guests who stayed at the resorts after 2017, and MGM said it is confident that no financial or password data was involved in the security incident.[v]

Iranian hackers have been taking advantage of major security bugs in a large number of enterprise VPN servers, such as those sold by Pulse Secure, Palo Alto Networks, Fortinet, and Citrix, to install backdoors in companies around the world. According to a report from cyber security firm ClearSky that was released in February, Iran's government-backed hacking units make it a top priority to exploit VPN bugs as soon as they become public. According to the report, Iranian hackers have targeted companies in IT, telecom, oil & gas, aviation, government, and the security sector, often within hours of a security bug becoming public.[vi]

The US Department of Justice announced charges against four Chinese hackers believed to be members of the Chinese People Liberation Army (PLA) for breaching US credit reporting agency Equifax in the summer of 2016.

The data breach, disclosed by Equifax in September 2017, involved the details of 145.5 million Americans, as well as millions of British and Canadian citizens. The quartet of hackers stole not only personal information, but also Equifax's proprietary data.

The DOJ had previously charged five other Chinese military hackers in 2014 for hacks against multiple US companies. In addition, the FBI said it is currently investigating more than 1,000 cases of Chinese theft of US technology.[vii]

Facial recognition startup Clearview AI said its full client list—which includes over 600 law enforcement agencies—was stolen. Intruders were able to learn how many accounts those agency set up, and how many searches they've conducted. Clearview said its servers weren't breached, nor was its database of three billion images, and that they were able to patch the vulnerability.[viii]



Evolve ETFs
Brookfield Place, 161 Bay Street, Suite 2700, Toronto ON M5J 2S1
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com

Clearview came under intense public scrutiny earlier in 2020 when a The New York Times revealed that Clearview built its facial recognition database by scraping publicly available photos from websites like Facebook, Instagram, YouTube and Venmo.[ix]

## PERFORMANCE ATTRIBUTION:

For February 2020, 21Vianet Group, Inc. was the best performing stock held by the Evolve Cyber Security Index Fund (CYBR), followed by VirnetX Holding Corporation and Zix Corporation. The Fund's largest exposure by weight was to Check Point Software Technologies Ltd., followed by Okta, Inc. and Fortinet Inc.

## SOURCES:


[i] https://www.bbc.com/news/technology-51474109
[ii] https://krebsonsecurity.com/2020/02/encoding-stolen-credit-card-data-on-barcodes/
[iii] https://www.tripwire.com/state-of-security/featured/puerto-rico-government-email-scam/
[iv] https://www.zdnet.com/article/fbi-bec-scams-accounted-for-half-of-the-cyber-crime-losses-in-2019/
[v] https://www.theguardian.com/technology/2020/feb/19/mgm-resorts-hotel-hack-data-breach
[vi] https://www.zdnet.com/article/iranian-hackers-have-been-hacking-vpn-servers-to-plant-backdoors-in-companies-around-the-world/
[vii] https://www.zdnet.com/article/doj-charges-four-chinese-military-hackers-for-equifax-hack/
[viii] https://www.engadget.com/2020/02/26/clearview-ai-client-list-exposure/
[ix] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html


## DISCLAIMER:





Evolve ETFs
Brookfield Place, 161 Bay Street, Suite 2700, Toronto ON M5J 2S1
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com