Nasdaq

January 2021

Fourth Quarter 2020 Update: ISE Cyber Security UCITS Index (HUR)

- Global equities ended the year on a high note, as the Nasdaq Global Index (NQGI), which is designed to track the performance of global equities covering over 98% of the entire listed market capitalization of the global equity space, gained 15.24% in the fourth quarter (Q4) of 2020. As a result of the strong finish, NQGI closed 2020 in positive territory, up 13.75%.
- The Technology industry maintained its momentum in Q4 2020, as the Nasdaq Global Technology Benchmark (NQG10) gained 15.37% in Q4 2020. In 2020, NQG10 gained 45.98%.
- The ISE Cyber Security UCITS (HUR) advanced higher in Q4, gaining 20.85% over the trailing three months. HUR gained 42.94% in 2020, beating the global benchmark, NQGI, by 29.19%, yet trailing the NQG10 by only 3.04%.
- The cyber security theme moved front and center in 2020, driven by catalysts such as the COVID-19 pandemic, the rise of remote work, escalating losses due to cybercrime, and the occurrence of one of the most sophisticated and most threating cyber breaches in recent years.
- At the height of the COVID-19 pandemic, "FBI reported its Cyber Division was receiving as many as 4,000 complaints per day about cyber-attacks, a 400% increase from pre-pandemic figures."[1]
- Crowdstrike, a cyber security infrastructure provider, reported in September, that "it had seen more intrusion attempts during the first half of 2020 than in all of 2019."[2]
- The increase in remote work and the work from home (WFH) movement in 2020 sparked a rise of cyber-attacks and vulnerabilities. According to Splunk, a cyber security infrastructure provider, a reported "47 percent of IT executives interviewed said cyberattacks were up since the pandemic began. More recently, 36 percent said they experienced an increased volume of security vulnerabilities due to remote work."[3]
- Records were broken in 2020 as cybercrime losses continue to escalate. According to the Washington Post, "Estimated global losses from cybercrime are projected to hit just under a record $1 trillion for 2020" which is "almost double the monetary loss from cybercrime than the $500 billion in 2018."[4]

[1] https://searchsecurity.techtarget.com/feature/Enterprise-cybersecurity-threats-spiked-more-to-come

[2] https://searchsecurity.techtarget.com/feature/Enterprise-cybersecurity-threats-spiked-more-to-come

[3] https://threatpost.com/2021-cybersecurity-trends/162629/

[4] https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.

- One contributing factor to the rise in cybercrime losses is the increase in ransomware “ransoms.” In 2020, the average ransomware requested fee increased to $200,000 from $5,000 in 2018.[5]
- In early December 2020, news of a massive, global supply chain attack (type of cyber attack where less-secure elements are exploited, often via tampering with electronics or systems in order to cause harm to parties involved further down the supply chain network). Hackers were able to exploit a “back door” in a Solar Winds, a leading provider of network monitoring tools, product.
- SolarWinds says at least 18,000 customers were impacted, some of which are important US government agencies and departments, such as the US Treasury Department, US Department of State, and even the Cybersecurity and Infrastructure Agency (CISA).[6]
- The supply-chain attack appears to have been first exploited back in March 2020 and suspected to be the work of Russia state backed hackers. According to Microsoft, who helped with the remediation of the attack, there has been a rise in “the determination and sophistication of nation-state attacks” and how “the attack appears to reflect a particular focus on the United States and many other democracies, it also provides a powerful reminder that people in virtually every country are at risk and need protection irrespective of the governments they live under.”

[5] https://www.wired.com/story/ransomware-2020-headed-down-dire-path/

[6] https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/) and https://www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/)

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.