Cybersecurity in Periods of Economic Contraction: Quantitative Findings

Cheaheon “Ian” Lim

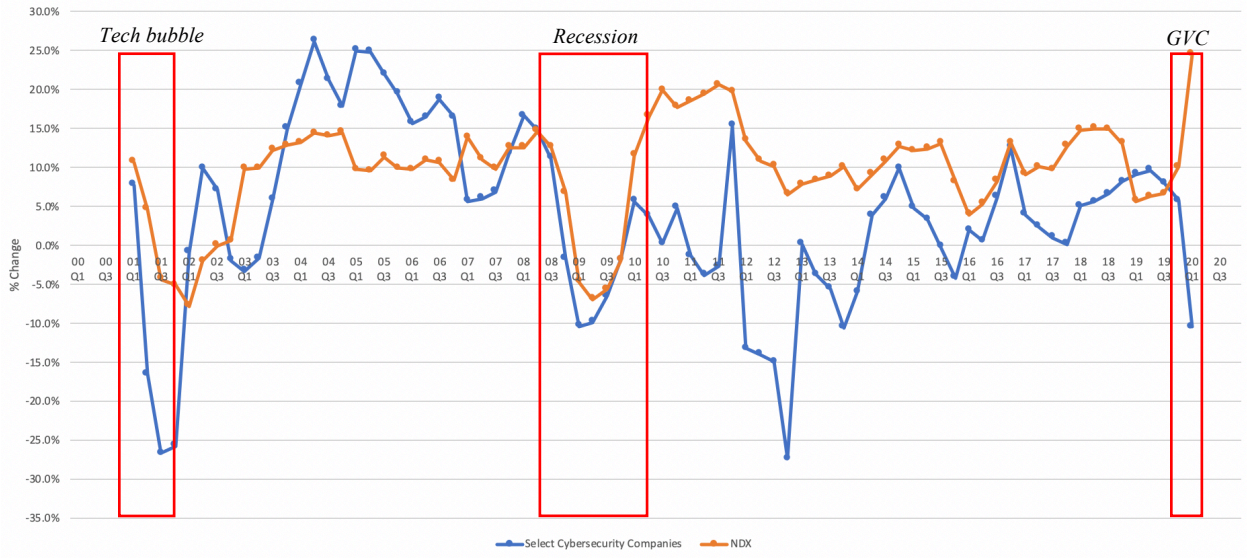
Version: 5.20.2020

I. Benchmarking Performance with QQQ

Methodology

To gain a preliminary understanding of the cybersecurity industry during periods of economic contraction, the YoY change in the average quarterly revenue of 35 publicly traded cybersecurity firms (partially sourced from First Trust Nasdaq Cybersecurity ETF, *CIBR*) were compared to that of companies in the Nasdaq-100 index.

Figure 1: YoY change quarterly revenue for cybersecurity firms versus NDX



Source(s): S&P Global Market Intelligence

Tech Bubble Burst and Great Recession

The average revenue of selected cybersecurity firms moved in line with that of Nasdaq-100 companies during the Great Recession, while the decrease in the annual revenue of cybersecurity firms were more pronounced in the quarters that followed the tech bubble burst. Such a phenomenon points to the fact that national cybersecurity spend may decrease not only in contractionary periods, but also in bearish markets when management seeks to widen margins in order to signal investors.

Great Virus Crisis (GVC)

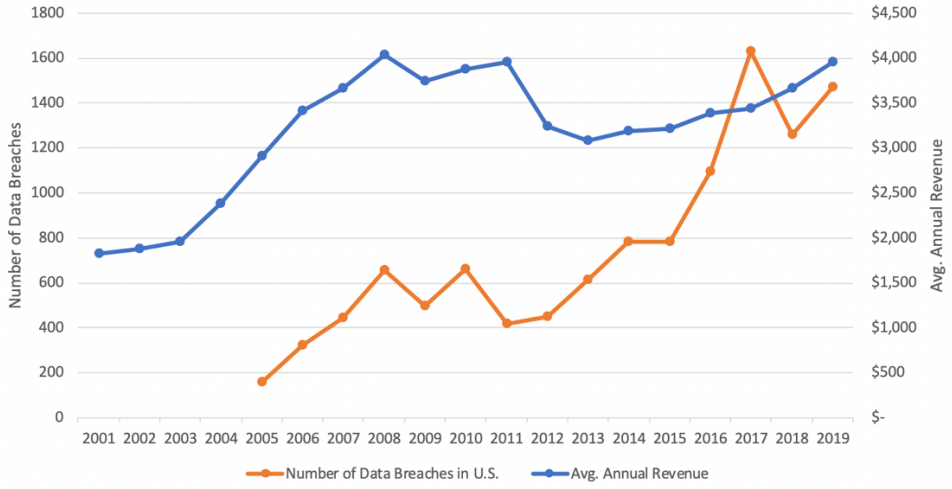
Government-mandated shelter-in-place measures began in late March, and as a result, the GVC did not have a significant impact on Q1 revenues for most Nasdaq-100 companies. However, even before COVID-19 started noticeably impacting firm-level operations in the last few weeks of Q1, many companies started implementing cost-cutting measures to bolster cash balances and brace for the GVC. Such actions most likely involved reducing spend on cybersecurity-related services, as is indicated by the noticeable ~10% YoY decline in the quarterly revenue of cybersecurity firms in Figure 1.

II. Modeling Annual Number of Data Breaches

Methodology

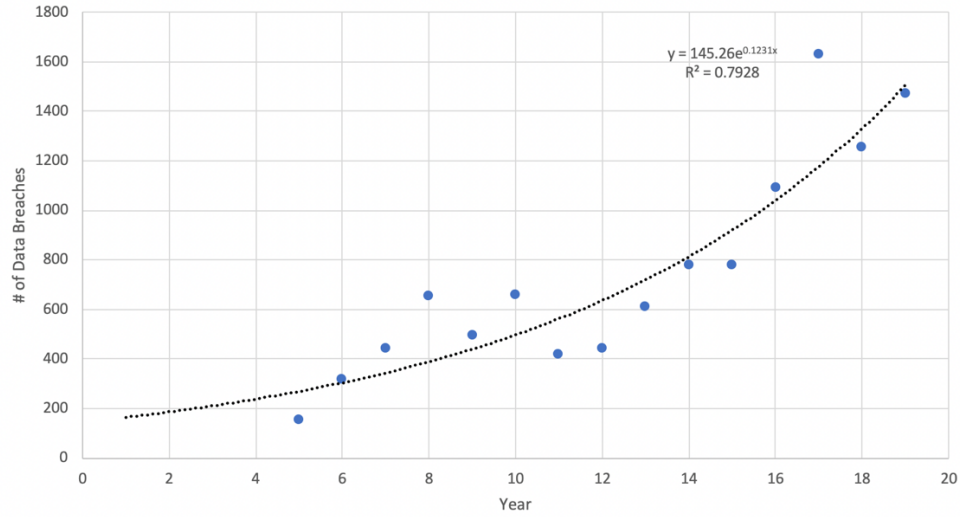
An exponential regression was performed on the annual number of data breaches in the U.S. with the underlying assumption that the number of cyberattacks experiences baseline organic growth YoY regardless of external factors—this makes intuitive sense as web-based technology increasingly becomes an integral part of most firms' operations. The present section seeks to determine the correlation between national spend on cybersecurity (revenue of selected cybersecurity firms used as a proxy variable) and deviations from model-driven expectations for the annual number of data breaches.

Figure 2: Selected Cybersecurity Firms' Avg. Yearly Revenue versus Number of Data Breaches in U.S



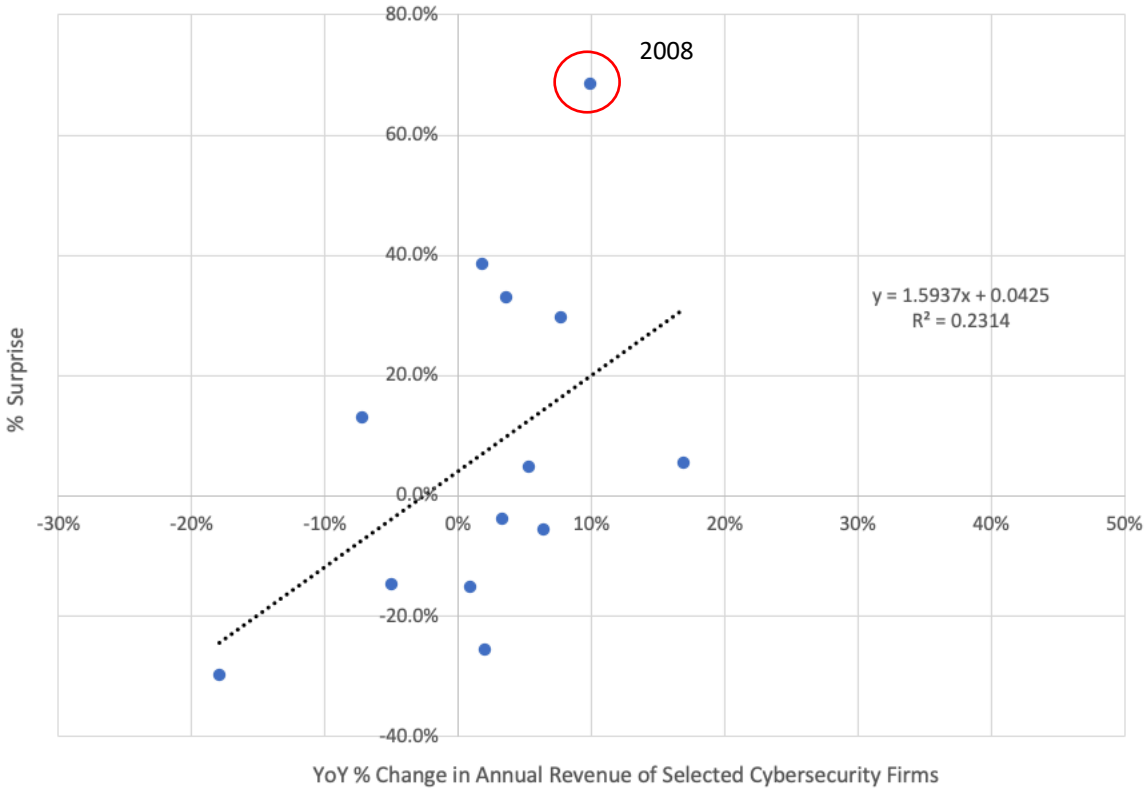
Source(s): Identity Theft Resource Center, S&P Global Market Intelligence

Figure 2: Number of data breaches in U.S. over time (2000-2019)



Source(s): Identity Theft Resource Center

Figure 3: % Difference in expected and actual # of data breaches as a function of YoY % change in avg. annual revenue of select cybersecurity firms



Source(s): Identity Theft Resource Center, S&P Global Market Intelligence

Exponential Model for Data Breaches

As can be seen in Figure 2, the annual number of data breaches in the U.S. closely follows an exponential growth model, where x denotes the number of years since 2000:

$$f_{expected}(x) = 145.25 * e^{0.123x}$$

Figure 3 demonstrates that there exists a noticeable positive correlation between the average annual revenue of selected cybersecurity firms and deviations from $f_{expected}(x)$, as defined by:

$$deviation = actual\ \#\ of\ data\ breaches - f_{expected}(x)$$
$$\%\ surprise = deviation / f_{expected}(x)$$

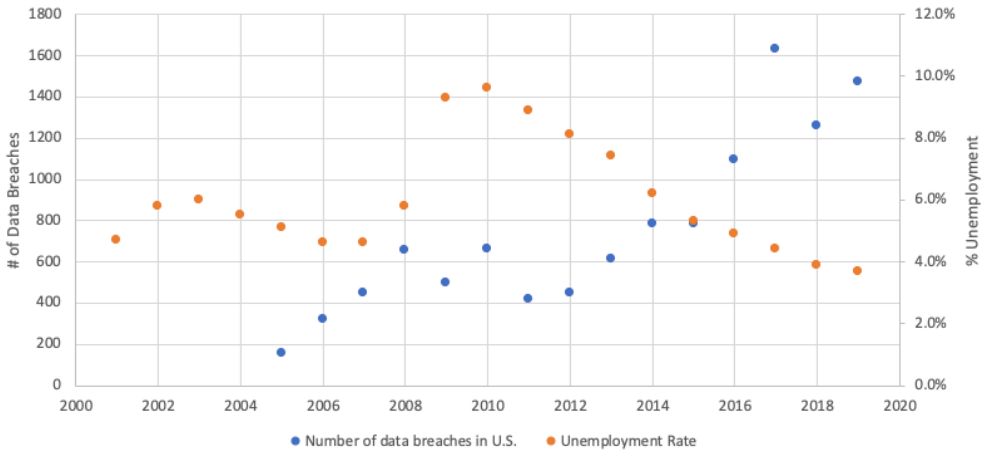
As can be seen, *% Surprise* is positively correlated with the YoY % change in revenue of selected cybersecurity firms, demonstrating that an increase in cybersecurity-related spending (i.e. increase in revenue of cybersecurity firms) may be a reactionary consequence of higher number of data breaches (i.e. higher *% surprise*) throughout a given year.

III. Correlation between Unemployment and Cybersecurity

Methodology

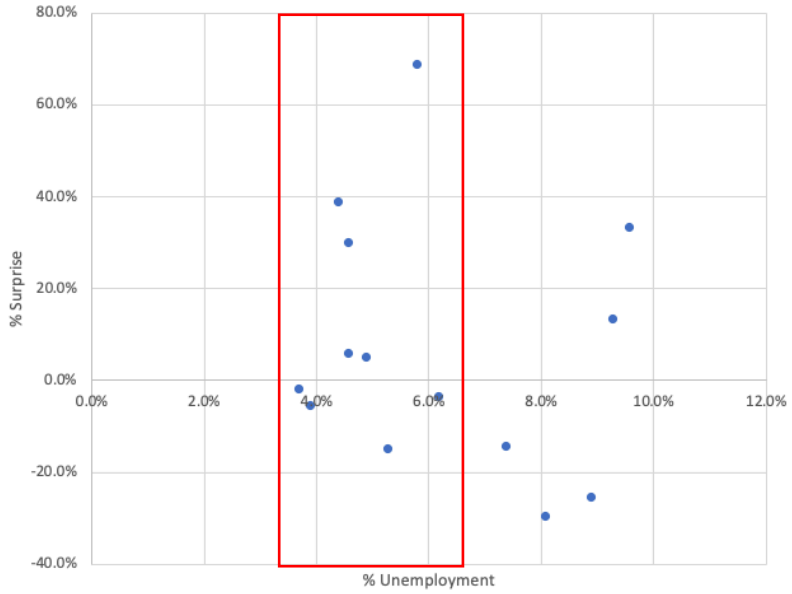
Section II demonstrated that the YoY % change in revenue of cybersecurity firms could not be used to model for *% surprise*, as the latter variable seemed to impact the former, rather than the other way around. In this section, the annual unemployment rate is used as a proxy variable to determine the potential existence of a causational relationship between the macroeconomic climate and *% surprise.*

Figure 4: Annual # of data breaches versus unemployment rate



Source(s): St. Louis Fed, S&P Global Market Intelligence

Figure 5: % Surprise as a function of annual unemployment rate



Source(s): St. Louis Fed, S&P Global Market Intelligence

Threshold Value for Annual Unemployment Rate

As can be seen in Figure 5, when unemployment rates are lower than 7.0%, there is a seemingly haphazard distribution of the *% Surprise* variable (datapoints inside red box). However, clustering analysis on the dataset revealed that a nontrivial correlation exists between unemployment rates and *% surprise* when the annual unemployment rate is greater than 7.0% (in years 2009, 2010, 2011, 2012, and 2013). Higher unemployment rates seemed to be associated with higher *% surprise,* as is indicated in Figure 6. Multiple studies on the macroeconomic climate and crime rates have revealed that in times of economic contraction, crime rates tend to be higher. Then, the derived relation in Figure 6 makes intuitive sense and may also imply that a causational relation exists between the two variables, where higher unemployment rates (when greater than 7.0%) are conducive to a higher *% Surprise* (which represents higher-than-expected number of data breaches in a given year).

Figure 6: % Surprise as a function of annual unemployment rate (modified ver.)