GuyCarpenter

DOUBLE-WHAMMY?

Examining the Correlation Between Major Cyber Events and Broad Market Performance

A business of Marsh McLennan

CONTENTS

Section 1

INTRODUCTION & METHODS

In Guy Carpenter's report, ***Through the Looking Glass: Interrogating the Key Numbers Behind Today's Cyber Market***, published in June 2023, we highlighted the importance of unlocking reinsurance capacity to fuel cyber market growth. Providers of alternative capital by way of insurance-linked securities (ILS) products are key sources of potential additional capacity.

However, despite the rapid expansion of cyber insurance market, ILS funds have been slow to enter the space. ILS investors' concerns around cyber insurance are two-fold: the relative nascency of commercial cyber models that poses a challenge to risk quantification, and the perceived correlation between cyber events and stock market performance.

As cyber catastrophe models are approaching a point of maturity and sophistication, their outputs are being increasingly relied upon by traditional reinsurers and alternative capital investors. Guy Carpenter's subsequent report, *Under the Lens: Investigating Cyber Vendor Model Divergence*, applies advanced predictive analytics to investigate the key drivers of cyber catastrophe model differences. That study aims to provide a level of comfort to cyber market participants in constructing their own views of exposure accumulation as their book of business expands and evolves.

This report addresses ILS funds' other concern around correlation between cyber events and the performance of the equity market, which, in turn, drives the performance of their investment portfolios. There is a long-held skepticism among the investment community that when a systemic cyber catastrophe event happens, it would result in a wide-ranging stock market downturn, since such an attack tends to be indiscriminate, and its victims would span across the entire economy. Many ILS funds are reluctant to deploy capital in cyber transactions for the fear of a "double-whammy" situation in the immediate aftermath of a widespread cyber attack.

In this report, a joint effort between the Guy Carpenter and Marsh McLennan Cyber Risk Intelligence Center teams, we evaluate extensive industry and academic research to demonstrate the lack of correlation between any observable historical cyber events and stock market performance. Our goals are to address ILS investors' concerns around the "double-whammy" situation and to provide investors and the broader insurance community with the data-driven support to make an informed decision about capacity deployment.

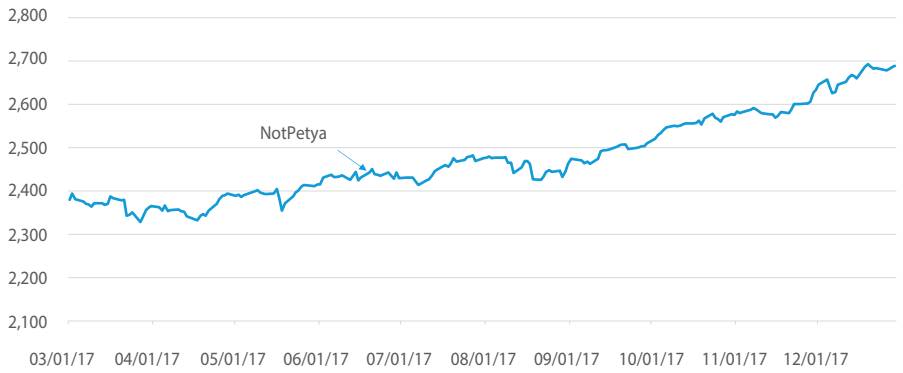
1. What is the question?

We wanted to understand to what extent, if any, historically large and impactful cyber events had any discernible effect on the stock market. Additionally, we wanted to use past events to inform what dynamics might lead a cyber-driven event to have a material stock market impact.

2. Evaluating historical events

We began our window of market analysis on January 1, 2000. We felt it was a long enough timeframe to be significant and to contain a large variety of events, yet recent enough to be relevant. For the evaluation of past major cyber events, we created a list of cyber events that have been considered "major," and broke them into 4 categories:

Figure 1. S&P Index Historical Prices

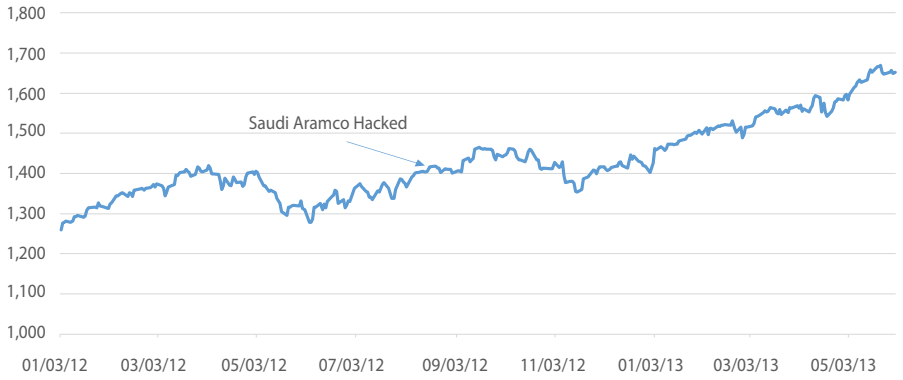


- Mass breach or vulnerability event
  - These are events that involve large-scale hacking campaigns, widespread vulnerabilities, or a combination of both. Solarwinds, Log4Shell, and NotPetya are recent examples.

Figure 2. S&P Index Historical Prices

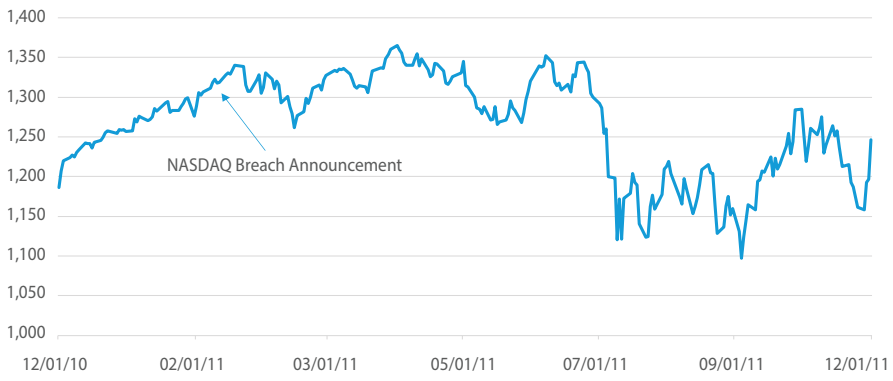
- Mass service outage
  - These are events that result in broad loss of availability for multiple companies. The April 2011 Amazon Web Services (AWS) outage, 2016 Dyn distributed denial of service (DDoS), and the 2018 O2 Cellular service outage are examples.

Figure 3. S&P Index Historical Prices



- Critical infrastructure compromise
  - These are events that impact a critical sector, such as energy or transportation. Colonial Pipeline, Saudi Aramco, and the August 2003 blackout[1] are examples.

Figure 4. S&P Index Historical Prices



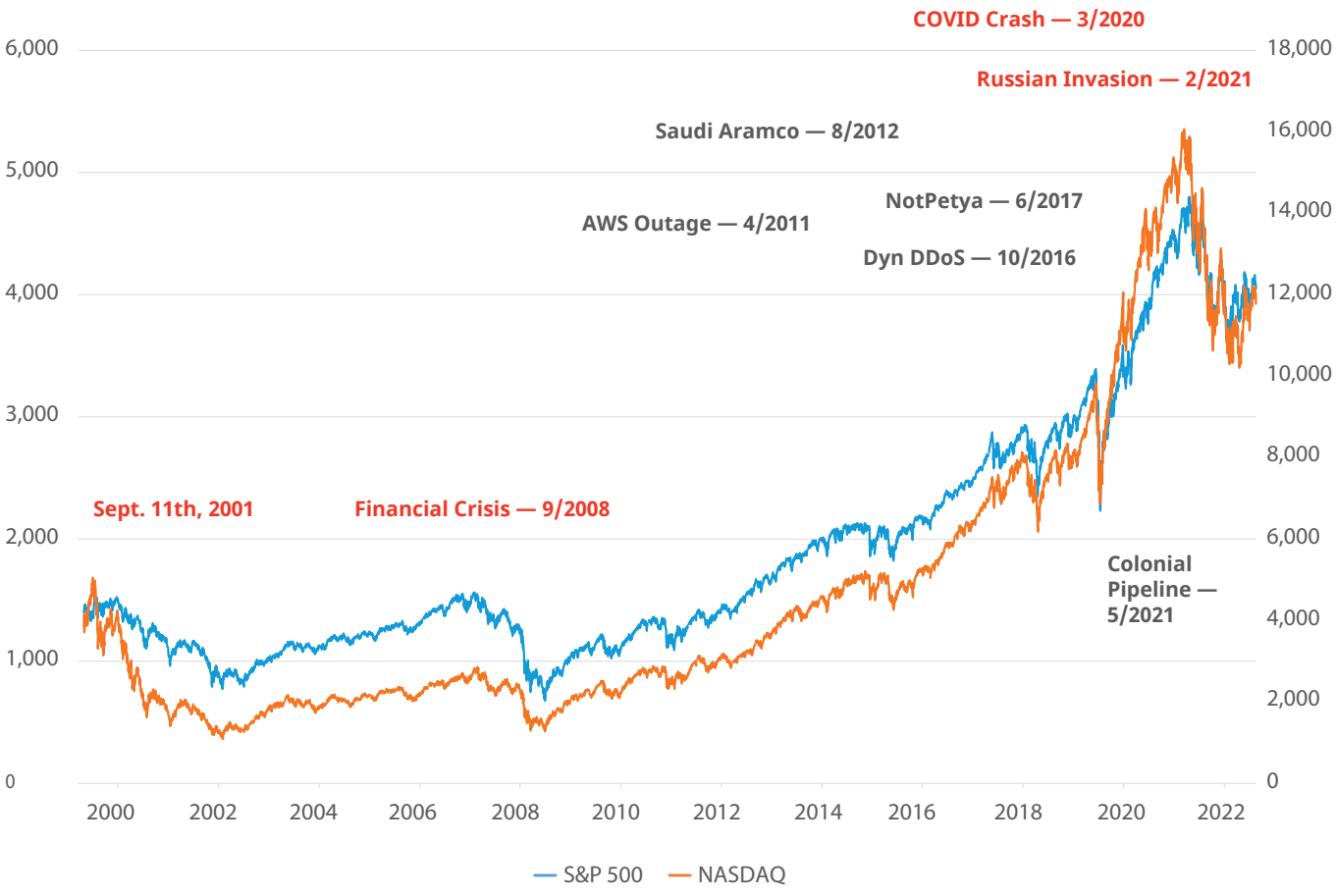
- Financial market compromise
  - These are events that indicate a compromise of the confidentiality, integrity or availability of financial and securities markets themselves. The 2010 NASDAQ breaches, the 2020 New Zealand Stock Exchange DDos attacks and most recently, the ION ransomware attack, are all examples.

Source: S&P Capital IQ Pro

In total, we generated a list of 14 major cyber events with distinct event dates. Importantly, the dates reflect when the markets became aware of these events, either through their direct impacts or via open-source reporting.

For comparison purposes, we chose 4 major events since 2000 that we know have had significant market impacts. We included the September 11, 2001 terror attacks, the Lehman Brothers' bankruptcy, the COVID-19 crash, and the Russian invasion of Ukraine as distinct events that preceded major market shifts. Each of these had different characteristics, but ultimately all had some significant effect on the market.

Figure 5. S&P 500 and NASDAQ, 2000-2023



Source: S&P Capital IQ Pro

3. Getting an answer

We wanted to know whether any major cyber events had any discernible effect on the markets, aside from the "normal" volatility for any given day. Therefore, our methodology was simply to compare the N-day post-event performance of any given cyber event against the larger population distribution of all days in the time window of January 1, 2000 to May 1, 2023. Again, as a comparison point, we also looked at the post-event performance of the 3 major non-cyber events listed above to show what a true effect would look like.

KEY OBSERVATIONS

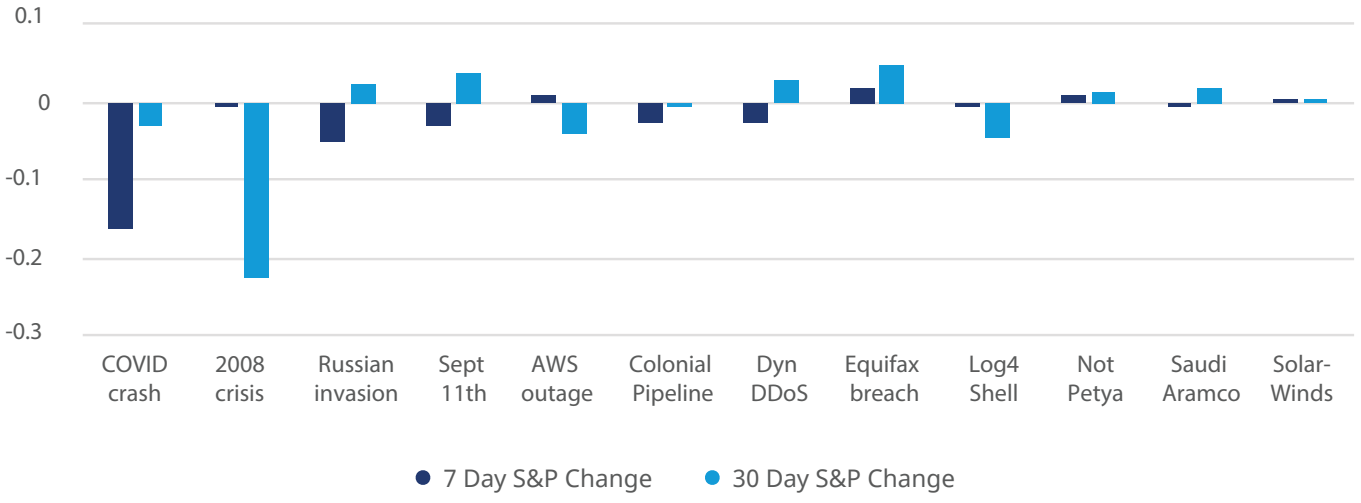
To test whether major cyber events had any significance to the S&P 500, we performed a simple p-test with a p value of .05. Essentially, this examines where, in the distribution of market returns, the periods immediately after cyber events appear. If the impact on market returns from a type of event is further than 95% out—a p value below 0.05—then it is conventionally considered significant rather than the result of financial market random noise.

When plotted against the distribution, the cyber events appeared close to the mean and certainly not far enough out into the tail to merit significance. This indicated that the effect of a cyber event falls within the random noise in the market.

	Known Impacting Events	Major Cyber Events	Outages
P value	0.014	0.446	0.212
Threshold	0.05	0.05	0.05
Significant?	YES	NO	NO

As a further exhibit, when examining the 7- and 30-day effects, we compare the 4 known impacting incidents with a sample of major cyber incidents:

Figure 6. S&P % Change, 7 and 30 Days Post Event

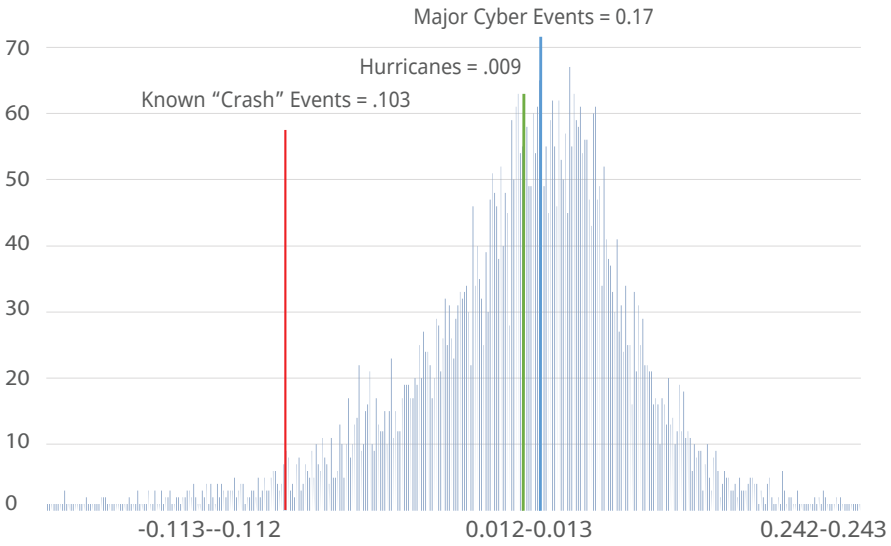


Source: S&P Capital IQ Pro

COMPARISON TO NATURAL CATASTROPHES

Because we were curious, we also added in 5 of the largest hurricanes of the past 20 years. The average 30-day performance of the S&P 500 after a cyber event is very similar to the results for hurricanes. This is not to say that cyber events and hurricanes are equivalent—they are not.

Figure 7. Frequency Distribution of 30-day Returns, S&P 500 2000-2023

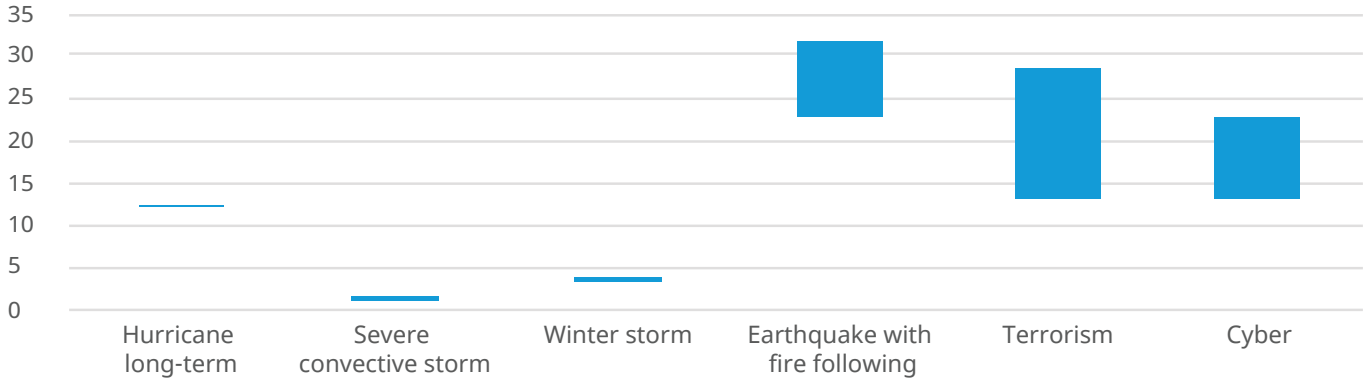


Source: S&P Capital IQ Pro

As seen in Figure 7, when plotted along the distribution of 30-day returns for the entire 2000-2023 time period, the broad market effect of major cyber events appears to be very similar to that of major hurricanes.

While the underlying systems and domains of natural catastrophes and major cyber events are different, it is possible to find similarities in their effects. For the most part, these events result in large one-time losses, not strategic shifts in economic activity or investment. This examination of the time dimension of impacts is discussed in later sections.

Figure 8. 200-Year Return Period Tail to Mean Ratio



Source: Guy Carpenter

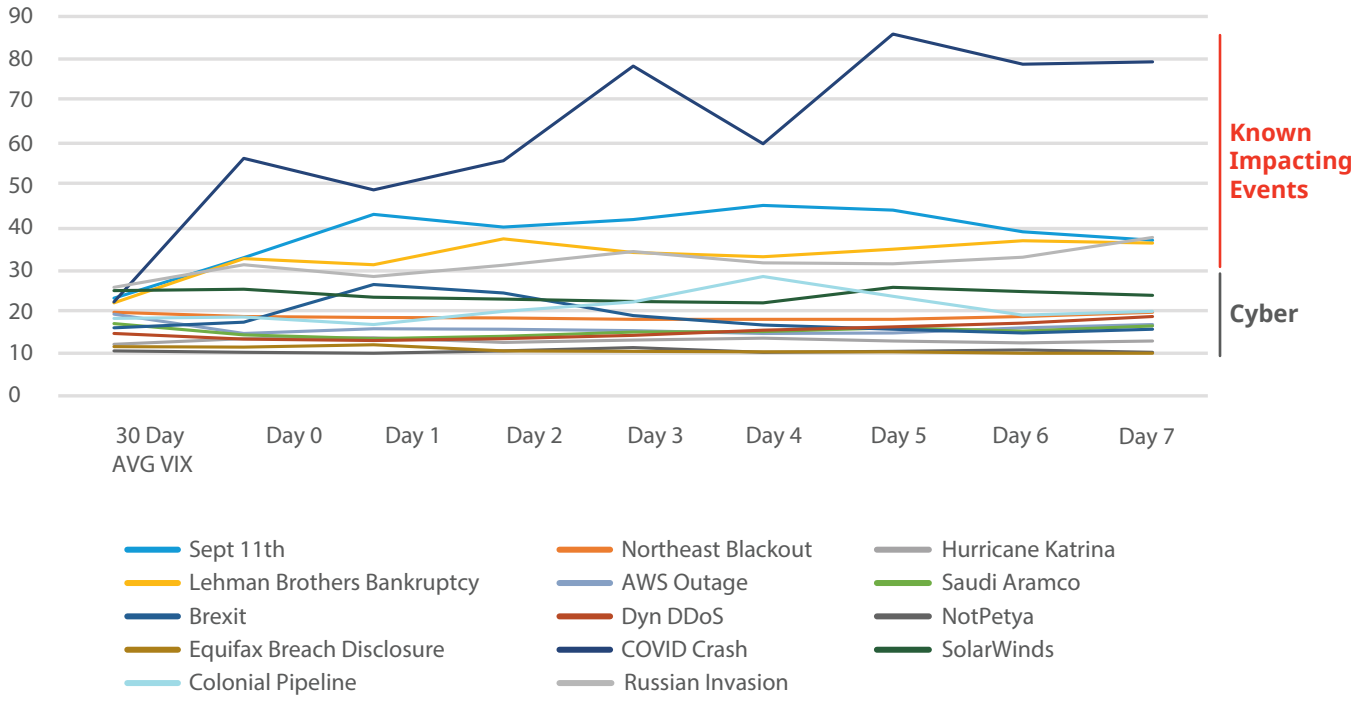
Looking beyond historical events, similarities also exist between natural catastrophes and cyber catastrophes from a modeling standpoint. Our investigative work in *Through the Looking Glass: Interrogating the Key Numbers Behind Today's Cyber Market* indicated that both cyber's modeled tail volatility and vendor model divergence are broadly in line with other, more-established catastrophe perils, particularly those with high severity and low frequency, such as earthquake. These results indicate that comparisons between cyber and natural catastrophes are relevant, and we can continue to draw meaningful inferences from them.

LOOKING DEEPER

In addition to looking at the "markets" using the S&P 500 as a barometer, we decided also to look at the VIX. According to Investopedia, "The CBOE Volatility Index, or VIX, is a real-time market index representing the market's expectations for volatility over the coming 30 days. Investors use the VIX to measure the level of risk, fear or stress in the market when making investment decisions."[2] While there is debate about the predictiveness of the VIX for large shifts in the market, historically there has been an 80% correlation between the VIX and the direction of the S&P 500.[3] We felt it might provide more insight into investor sentiment.

How did these events affect the VIX?

Figure 9. VIX, First 7 Days Post-Event



Source: S&P Capital IQ Pro

"The long-run average of the VIX has been around 21. High levels of the VIX (normally when it is above 30) can point to increased volatility and fear in the market, often associated with a bear market."[4] As indicated above, the VIX has only breached 30 in our dataset for the known, high-impacting, non-cyber market events. None of the cyber events led to meaningful rises or shifts in the VIX, with Colonial Pipeline setting the high-water mark of the cyber events at 27.59 on Day 4.

CONCLUSIONS

The lack of a broad market effect does not mean these events were not impactful. Quite the contrary—they were deeply impactful to the victims involved, as well as, in some cases, to large parts of the economy.

- The final tally on NotPetya's damage equaled USD 10 Billion.[5]
- Saudi Aramco's networks were down for close to 5 months.[6]
- It is suspected that the Colonial Pipeline hack led to an increase of 4 cents per gallon in the price of gasoline.[7]

Why then, did the markets not meaningfully react?

It is useful to remember that, as NASDAQ points out: "The stock market is not the economy."[8] Furthermore, it is important to note that the performance of, say, the S&P 500 is driven by **expectations**, not the current state of affairs. That is to say, as economist Dean Baker writes, "The stock market tells us about the expected value of future after-tax corporate profits."[9]

In this lens, external events need not only be impactful in the moment but also impact the direction that corporate revenues might go in the future. An albeit-large one-time cost to a company, or even many companies, as we saw with NotPetya, may still not materially impact their operations and future revenue streams enough to create a market sell-off. Large business interruptions from outages may similarly incur huge losses, but they do not meaningfully change the course of business for the impacted entities. In order to enter the class of catastrophe that can trigger a bear market, it is possible that cyber events must "escape" to the larger domains of financial and economic activity—impacting the movement of people, products or money.

Imagining how a cyber event might directly, or via contagion, cause these effects is not difficult. In fact, short-term impacts to transportation systems, such as the US Federal Aviation Administration (FAA), financial infrastructure, such as the Society for Worldwide Interbank Financial Telecommunications (SWIFT), and even cyber-induced supply-chain slowdowns have indeed all occurred and yet have not hit the potential thresholds necessary to incur market impacts. Determining where these thresholds might lie and how likely they are to be breached via cyber means is the subject of future research.

FUTURE WORK

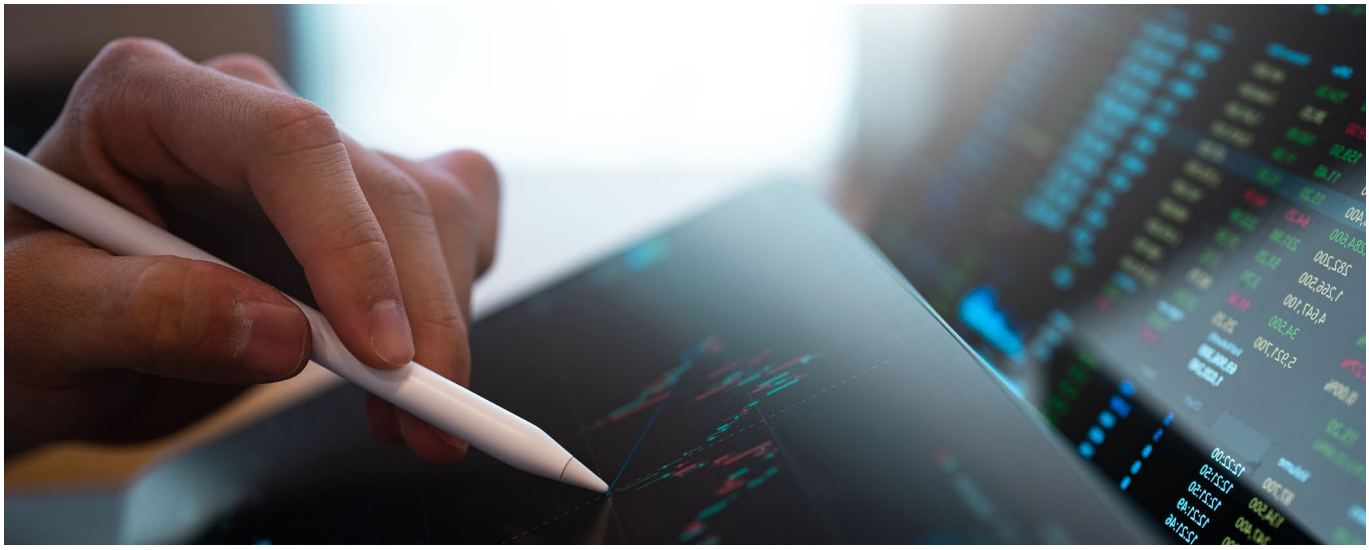
In *Dismissing Cyber Catastrophe*, James Lewis of CSIS writes, "It is easier to imagine a catastrophe than to produce it." Cyber catastrophes of various types have been predicted for decades. While many of the previously unimaginable scenarios have now indeed occurred (ransomware and wiper worms, grid and pipeline attacks, market disruptions, electoral interference, etc.), none of them has evidently produced broader impacts, at least in the financial markets.

On the other hand, we can examine the counterfactuals of past event paths and theorize what might have happened if outages had lasted longer or malware had spread further. Here, too, the probabilities get tricky. Historically, outage durations drop off significantly after 48 hours, and even inferring a probability from a smoothed distribution yields remote percentages. Malware spread is often limited by software and operating system (OS) footprints, not to mention the complexities of modern networking and platforms. Furthermore, controls that become available should they be necessary—redundant systems, government intervention, manual operations—have several times mitigated the contagion of large-scale cyber events.

Lewis also writes, "One major failing of catastrophe scenarios is that they discount the robustness and resilience of modern economies." Even under counterfactual scenarios when a catastrophic cyber event might "escape" into the broader economy and impact investor confidence, there are non-cyber defenses that may contribute to a response and ameliorate concerns. Further research and modeling are needed to examine these counterfactual scenarios and understand what reasonable inferences we can make about likelihood.

In subsequent releases, we hope to outline various frameworks for thinking about cyber catastrophes—the causes, historical datasets and inter-system dependencies that could contribute to contagion effects. We also hope to inform reasonable likelihood estimations for severe events that may not have yet occurred. We will continue to investigate parallels between cyber and natural catastrophe perils, both from an actual incident and model development standpoint.

We aim to help ILS investors and the broader insurance community improve their understanding of the cyber catastrophe landscape, so instead of viewing cyber risk with fear and uncertainty, the industry collectively will be more confident about deploying capital on cyber.



OPPORTUNITY FOR ILS

As of today, ILS investors have participated in several excess of loss collateralized reinsurance transactions covering cyber risk, generally on a private and limited basis in terms of capital deployed.

One of the hurdles has been that ILS funds and their end investors have taken a view that cyber risk correlates to financial market risk, which has led to limited capital deployed to date due to the potential "double-whammy" scenario.

Views of natural catastrophe risk—for example, earthquake and hurricane insurance risk not correlated to stock market risk and therefore producing non-correlating returns—has been key to investors placing capital into this (re)insurance risk asset class. (Re)-insurance risk is appealing to investors when a) the risk adds diversification benefit to their overall asset portfolio and b) provides adequate returns above the risk-free rate.

Our analysis and results in this report provide evidence that historical widespread cyber events, such as Microsoft Exchange, or those targeted at critical infrastructure, such as the Colonial Pipeline, have had no lasting or significant impact on stock market performance, a similar dynamic to when natural catastrophe events occur. In fact, the average 30-day performance impact of the S&P 500 after a cyber attack is very similar to when major hurricanes have occurred.

Generally, markets have not seen or priced in long-term negative impacts in individual companies' share prices or across industry verticals after cyber events due to sophisticated and fast remediation efforts and consequently the ability to "bounce back" to rectify specific issues limiting collateral damage.

In fact, like natural catastrophe risks, cyber risks are contained to the footprint of the exposed target—for example, an outage of a large cloud service provider should only affect the customers of that provider.

However, unlike natural catastrophe events, the impact of cyber catastrophe events can be limited and reduced with human intervention and artificial intelligence (AI) cyber management tools, such as identifying vulnerabilities that are exploitable due to a zero-day vulnerability and then patching them.

Furthermore, with appropriate structure mechanics, agreement across all parties around what scenarios/events are subject or covered under a cyber catastrophe transaction, along with risk modeling to reflect this, cedents and investors will be in a stronger, more confident position to engage and transfer cyber risk.

In conclusion, this presents an opportunity for investors who have invested in natural catastrophe ILS to diversify their existing portfolios further, and for those who have not entered the natural catastrophe ILS market to invest in a sophisticated and growing area of (re)insurance risk.

The size and relevance of the cyber (re)insurance market has increased substantially in the past decade, supported by traditional reinsurance capacity, and it is now looking for a scalable, diversified capital base to unlock future growth. ILS investors are ideally suited to be key capital partners for cyber (re)insurers, bringing new capital into the ecosystem. ILS investors have historically demonstrated the ability to undertake a broad range of risks, and cyber continues to be a key opportunity and developing area of interest.

CONTACTS

Anthony Cordonnier
Global Co-Head of Cyber
anthony.cordonnier@guycarp.com

Erica Davis
Global Co-Head of Cyber
erica.davis@guycarp.com

Zain Hussain Awan
International Cyber ILS Lead
zain.awan@guycarp.com

Additional contributors:

Matt Berninger

Jess Fung

References

[1] While not strictly a cyber-caused event, the 2003 blackout contained cyber elements related to its contagion and serves as an illustrative example.

[2] https://www.investopedia.com/terms/v/vix.asp

[3] https://www.cboe.com/insights/posts/inside-volatility-trading-breaking-down-the-vix-index-and-its-correlation-to-the-s-p-500-index/

[4] https://www.investopedia.com/terms/v/vix.asp

[5] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[6] https://money.cnn.com/2015/08/05/technology/aramco-hack/

[7] https://news.ku.edu/2021/12/16/cyberattack-colonial-pipeline-affected-gas-prices-far-less-initially-reported-study-finds

[8] https://www.nasdaq.com/articles/the-stock-market-is-not-the-economy

[9] https://cepr.net/the-price-of-wheat-doesnt-tell-us-about-the-strength-of-the-economy-and-neither-does-the-stock-market-why-is-this-so-hard-for-intellectual-types-to-understand/

GuyCarpenter

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with 3,400 professionals in over 60 offices around the world. Guy Carpenter delivers a powerful combination of broking expertise, trusted strategic advisory services and industry-leading analytics to help clients adapt to emerging opportunities and achieve profitable growth. Guy Carpenter is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. The Company's more than 85,000 colleagues advise clients in 130 countries. With annual revenue of over $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses including Marsh, Mercer and Oliver Wyman. For more information, visit www.guycarp.com and follow us on LinkedIn and Twitter @GuyCarpenter.

This document or any portion of the information it contains may not be copied or reproduced in any form without the permission of Guy Carpenter & Company, LLC, except that clients of Guy Carpenter & Company, LLC need not obtain such permission when using this report for their internal purposes.

Securities or investments, as applicable, are offered in the United States through GC Securities, a division of MMC Securities LLC, a US registered broker-dealer and member FINRA/NFA/SIPC. Main Office: 1166 Avenue of the Americas, New York, NY 10036. Phone: (212) 345-5000. Securities or investments, as applicable, are offered in the United Kingdom by GC Securities, a division of MMC Securities Ltd., which is authorized and regulated by the Financial Conduct Authority. Securities or investments, as applicable, are offered in the European Economic Area by GC Securities, a division of MMC Securities (Ireland) Ltd., which is authorized and regulated by the Central Bank of Ireland, reference number C447471. Main Office: Charlotte House, Charlemont Street, Dublin 2, D02 NV26, Ireland. Reinsurance products are placed through qualified affiliates of Guy Carpenter & Company, LLC. MMC Securities LLC, MMC Securities Ltd., MMC Securities (Ireland) Ltd, and Guy Carpenter & Company, LLC are affiliates owned by Marsh & McLennan Companies. This communication is not intended as an offer to sell or a solicitation of any offer to buy any security, financial instrument, reinsurance or insurance product.

©2023 Guy Carpenter & Company, LLC. All Rights Reserved.

1166 Avenue of the Americas, New York, NY 10036 I +1 (917) 937-3000