



Modeling a Cyber Catastrophe

Counting the Cost of a Major Email Service Provider Outage in the UK

JUNE 2019

BY MARCO LO GIUDICE & SHALOM BUBLIL

COUNTING THE COST OF A MAJOR EMAIL SERVICE PROVIDER OUTAGE IN THE UK

By Marco Lo Giudice & Shalom Bublil

Executive Summary

The cyber books of many (re)insurers may be modest; however, their potential exposure to a cyber catastrophe could be very large.

Even though overall cyber premiums are significantly lower than property in the UK, this report demonstrates that the potential for a multi-billion dollar insured loss is similar to the risk of floods catastrophes covered by property insurance.

Every day 290 billion email messages are sent worldwide by 3.9 billion users, facilitating a \$15 trillion global economy comprised of over 150 million organizations. Email is an integral critical business service for organizations operating in the digital age. Businesses use email to communicate internally with staff and externally with their customers, clients, partners, and supply chain. Behind these huge numbers are a small number of email service providers (such as Microsoft, Google, and Rackspace) that account for the majority of all emails sent. This presents a potentially disastrous risk to the availability of this essential service if one was to suffer an outage as the result of a cyber-attack.

A cyber-attack on an email service provider lasting hours, days or weeks and the resulting outage would lead to a substantial financial impact on a (re)insurance carrier. The key characteristics of this type of cyber catastrophe are high severity and low frequency, meaning, an event that does not occur regularly but entails great damage potential, effecting numerous businesses and leading to multiple claims on a (re) insurance carrier at a single point in time.



The financial damage caused by a cyber catastrophe, such as an email outage, could also manifest through silent risk. Regulators are increasing requirements to quantify this potential silent cyber risk. In January 2019 the PRA (Prudential Regulation Authority that regulates the UK Financial Services market (inc. the insurance market) demanded that UK insurance firms should seek risk models and expertise to estimate the potential silent (non-affirmative) cyber exposure across their portfolios and introduce robust mitigation strategies for limiting any potential risks.

This report examines an attack on an email service provider in the UK leading to a service outage resulting from a single point of failure, an event that can lead to financial damage and claims due to affirmative cyber coverage. In this report the authors utilized Kovrr's ability to quantify potential exposure to cyber catastrophes based on the composition of specific portfolios. Kovrr's predictive modeling platform was used to map the underlying technologies and services used by the insured companies, enabling an understanding of the potential accumulation risks that are derived from the aggregation of their network of utilised technologies and service providers.

Data Wipe Case Study: VFEmail.net

On the 11th February, 2019, hackers breached the servers of the email provider VFEmail.net and deleted all the data from its US servers, destroying all US customers data in the process. Users with VFEmail accounts were faced with empty inboxes and left with no recovery backup options. This was not the first occasion that VFEmail had been targeted. In 2015, VFEmail suffered a DDoS (Distributed Denial of Service) attack after the owner declined to pay a ransom demand from an online extortion group. The company was also forced to find a new hosting provider after a series of DDoS attacks in 2017.

Anatomy Of An Attack

An attack on an email service provider, larger than VFEmail, could result in critical data being held hostage, altered or destroyed for multiple organizations. This analysis reflects the financial loss resulting from this large-scale business interruption event and the insured loss due to insurance claims that would be triggered in the event of an email service provider outage. In order to perform this analysis, we simulated multiple events including an email service provider outage attack. For each event, we analyzed it's technical characteristics and calculated the estimated potential losses.




In the specific scenario modeled in this report, a cyber attacker is seeking to cause a large-scale service shutdown through a targeted attack on an email service provider.

The attack methodology chosen is based upon the Dyn / Mirai DDoS cyber attack of 2016. A Distributed Denial of Service (DDoS) is the type of attack where multiple compromised systems, are used to target a single system causing a Denial of Service (DoS).

In this scenario a service provider is taken offline via a large scale DDoS attack resulting in the providers' core services, being unavailable to its client base. The DDoS attack is performed via a large number of internet-connected devices (e.g. IoT devices) acting as a botnet.

These IoT devices have been compromised through self-propagating malware which finds, attacks and infects vulnerable devices through exploiting security weaknesses such as default usernames and passwords.

IoT DDoS Attack Methodology

80k IoT Devices Infected	180k IoT Devices Infected	240k IoT Devices Infected	440k IoT Devices Infected	630k IoT Devices Infected	770k IoT Devices Infected		
DAY 1	DAY 2	DAY 3	DAY 4	DAY 5	DAY 6	DAY 7	
Botnet growth through promulgation of IoT malware				DDoS attack starts targeting service provider with traffic estimated at 1 TBPS*	08:00am. Attack increases severity with addition of more botnet devices. Service provider services downgraded taking emails 120mins to send.	10:00am. Attack grows to 1.6 TBPS, additional servers affected. Email traffic is stopped, client unable to receive or send emails.	Attack continues for 72hrs. During 52hrs of the attack almost all clients of the email service provider lost access to their email service causing wide spread interruption to businesses.

* TBPS terabytes per second. Data based upon the DDoS attack initiated by the Mirai botnet against the hosting provider OVH. OVH reported that these attacks exceeded 1 TBPS, the largest on public record.

The Analysis Process

The findings of this report are derived from the results of a potentially catastrophic cyber event, modeled on a statistically representative portfolio of 40,000 UK companies and extrapolated to capture the overall implications on the UK market.

To understand the technologies used by the companies modeled, each business was analyzed to map the technology stack and service providers used to power its commercial operations. The results have considered the effects and resulting implications for different businesses within the dataset. Different business sectors reliance on email services and the effect of profit loss due to the inaccessibility of those services is the basis of the modeled vulnerability curves.

We also took into account multiple factors, including the controls that might limit the potential effects of a business's transaction frequency.

UK Portfolio Composition Overview

We leveraged a proprietary Industry Exposure Database (IED) containing data on all businesses currently operating within the UK. The dataset is a representative sample of businesses of different sizes, geographical locations, industry sectors, and turnover.

The median revenue of \$33 million is representative of the businesses within the dataset model commensurate with a book of UK insurance carriers composed of varying business sizes.

This figure is comprised of a small number of big enterprises with a large turnover, only 2% of the businesses in the dataset have a turnover above \$195 million.



Analysis: Modeling The (Re)Insurance Implications Of An Email Service Provider Outage

Exposure

The analysis shows 47% of businesses use one vendor in particular. The high concentration of UK businesses using this one vendor provides an excellent example on which to model the potential implications of a cyber catastrophe targeting such a crucial platform.

The modeled hazard was mapped through Kovrr's "provider reliance" index. Using this index we factored in the different service providers used by businesses in the portfolio, including the contribution each service provider makes to critical business processes.

Additionally, we mapped potential damage factors based on vulnerability curves that estimated the local severity of an event. These events took into account the specific procedures and processes that are core to each business's mission and the way they are organised to drive productivity.

Estimated Losses To The UK Market & The Insurance Gap

Economic Loss

\$44 Billion

The economic loss estimate for the cyber event with a three-day email service outage for the entire active companies in the UK is **\$44,559,367,816**.

Ground Up Loss

\$4.9 Billion

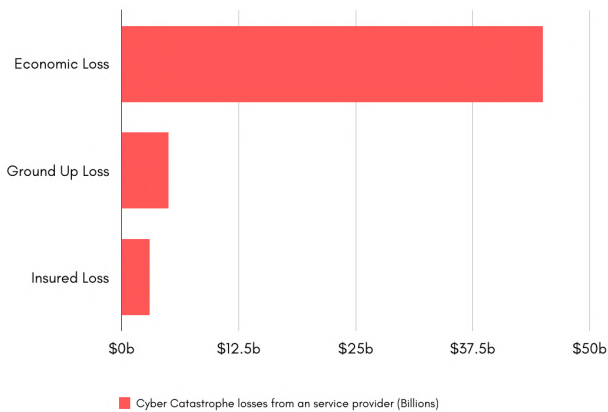
The economic impact of the event, the ground up loss, is **\$4,900,000,000** before terms and conditions (limits of the policy, deductible and waiting period).

Gross Insured Loss

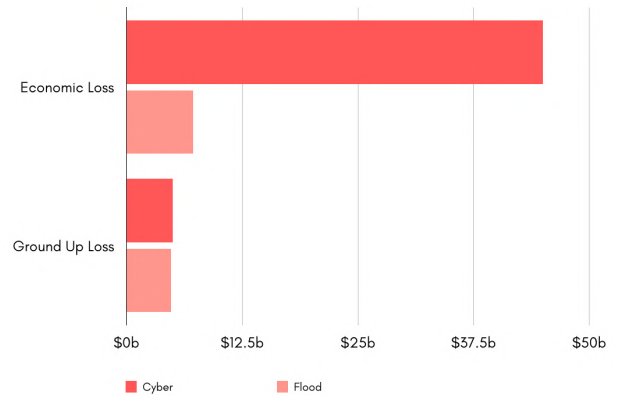
\$3.25 Billion

The gross insured loss is **\$3,235,010,103**. This figure was estimated by taking into account insurance adoption rates as well as the terms, conditions and average waiting periods before business interpretation coverage is activated.

Cyber Catastrophe Losses



Comparative UK Catastrophe Model: Property vs Cyber



The total insured loss from this scenario is similar to the 2007 property flood loss, which cost \$4.8 billion, across two events that occurred in June and July.

These events were a watershed moment for the UK insurance industry, spurring a number of initiatives aimed at better managing flood risk. In a similar fashion, as the cyber insurance market evolves and overall premium income increases, the potential insured losses will also grow accordingly.

The sizeable gap between insured loss and economic loss in our scenario is an indicator of the great potential for growth. Across all industries, decision makers are looking for coverage tailored both in type and size to their needs, while insurers are striving to provide such coverage; the key ingredients enabling demand and supply to meet are effective exposure management and catastrophe modeling. Such an insurance gap clearly indicates there is a great opportunity to fulfill an unsatisfied demand that exists for cyber insurance products.

Additional Considerations:

Catastrophe Modeling

Cyber risk modeling provides (re)insurers with the capability to accurately assess, quantify and stress test their potential catastrophic events exposure within their portfolios.

Allowing the (re)insurer to implement an underwriting and exposure management strategy based on a constant flow of real-time data rather than on top down assumptions alone.

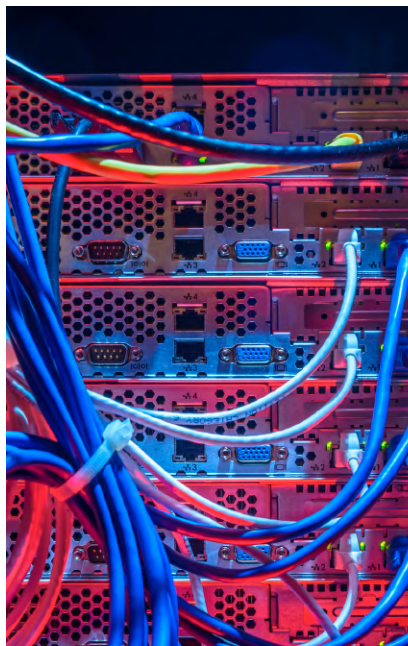
Enhanced management of such accumulations will enable exposure managers and catastrophe modelers to improve underwriting accuracy and better manage potentially catastrophic events.

It's also clearly more palatable than the alternative of onboarding and accumulating unknown risks. In comparison to other lines of business such as property or E&O, the current cyber protection gap creates a opportunity to grow cyber books and their wider business.

Silent Cyber

This report recognizes the potential impact of both affirmative and silent cyber risk.

When insurance policies do not explicitly exclude cyber risk, there's the potential for a cyber event to trigger business interruption claims. There is, therefore, the potential for claims from multiple other lines of insurance policies such as property and E&O which could in turn lead to potentially significant losses.



Regulatory

Understanding the adherence of the supervised carriers to regulatory requirements allows reinsurance and insurance companies to better communicate how they manage risk, by the stress tests conducted on their portfolios. This is especially true in regulatory environments such as the one in the UK where there are concerns about the potential effects of a cyber catastrophe that may lead to payouts in excess of a 1:250 years event.

Furthermore, the PRA is shining the spotlight on the potential damage of cyber exposures, specifically focusing on silent cyber risk.

Regulators are now asking (re)insurers for clear action plans to measure areas such as silent cyber risk. These developments should prompt (re)insurance actors to carefully invest in meeting and satisfying these new regulated guidelines as they continue to evolve.

Conclusion

The exponential growth and utilization of technologies are creating new paradigms of wealth creation and commercial opportunity. However, this brave new world is not without its dangers. The same platforms, services, and tools that power global trade and communication come with their own threats and vulnerabilities.

This report has sought to give shape to an example of cyber catastrophe and show the potential multi-billion dollar losses due to insurance claims arising from a single event affecting multiple businesses and leading to a significant loss. By utilizing proven methodologies consistent with other lines of catastrophe modeling and adapting them to model cyber events.

This report shows that by utilizing such an approach (re)insurers will be able to identify the potential risk accumulation within portfolios as well as identify opportunities to diversify risk exposure, adjust loss projections and improve their capital reserves. This will ultimately enable more effective management of tail risks; a critical capability for those operating in such a dynamic risk landscape.

About Kovrr

Kovrr is a predictive cyber risk modeling platform that enables (re)insurers to transparently predict and price single, accumulated & catastrophic cyber risk.

The Kovrr platform is designed to help underwriters, exposure managers and catastrophe modelers understand, quantify and manage cyber risk by utilising AI-powered risk models that continuously reflect new cyber threats.

To learn more please contact the Kovrr team:
contact@kovrr.com

The Authors



Marco Lo Giudice is SVP, Pricing at Renaissance Re and a member of Kovrr's Advisory board.



Shalom Bublil is one of Kovrr's co-founders and their Chief Risk Officer.

Kovrr's Yakir Golan, Naomi Weisz, Avi Bashan, Amir Kessler & Tom Boltman also contributed to this report.