KOVRR
Cyber Risk Modeling

www.kovrr.com

CRIMZON™
The Data Behind the Framework

NOVEMBER 2020

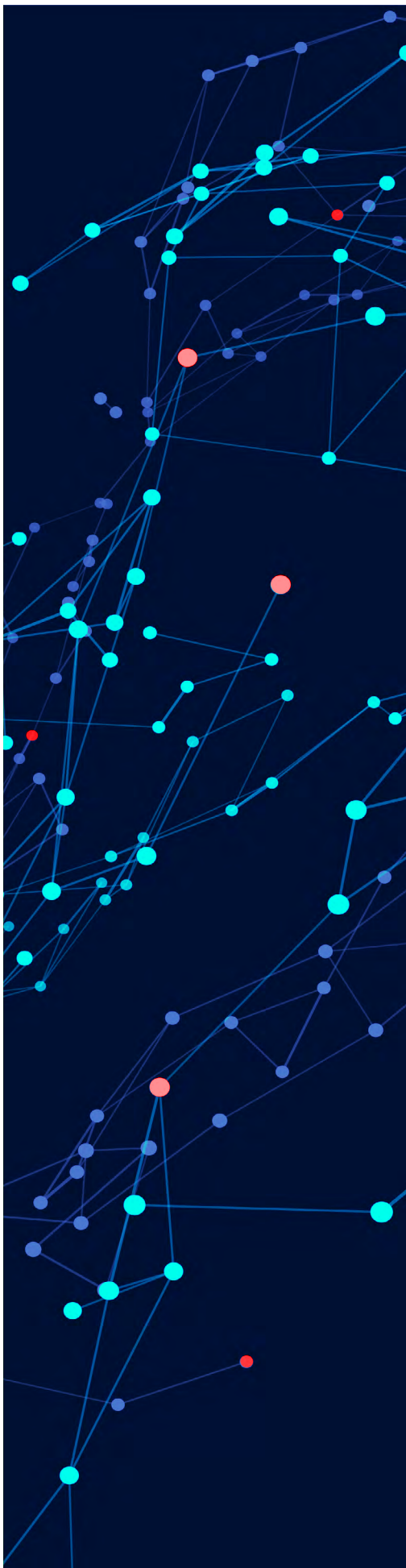
KOVRR
Cyber Risk Modeling

Abstract

The CRIMZON™ framework defines the minimal elements needed to provide a view of accumulated cyber risk. For natural catastrophe risk, individual policy exposures can be aggregated within geographic zones. Similarly, cyber exposures can be aggregated using CRIMZON. Location also holds importance when assessing cyber catastrophe risk, however, two additional elements must be taken into account to properly assess cyber risk accumulation: industry and company size. Insured companies with common characteristics related to location, industry, and entity size tend to be exposed to similar types of cyber events because these elements also correspond to technologies or service providers used. Based on an analysis of millions of cyber events in the last 20 years, Kovrr conducted extensive research, to serve as the core empirical validation for the CRIMZON framework. Below is a subset of the research, in which a study group of 120 CRIMZON was determined by selecting CRIMZON with the highest relevance to the cyber insurance market.[1] The total number of unique companies in the study group is 20,000, with an average number of 152 companies within a CRIMZON, and a median of 86 companies. The research criteria focused on companies' location industry, entity size, and the hosting and mail technology and service providers used by companies. The results showed a concentration of technologies and services when grouping by location, and further concentration when adding the additional elements of the CRIMZON, entity size and industry to the analysis. The research shows that companies within the same CRIMZON have the tendency to use the same service providers and technologies, and that different compositions of service providers and technologies can be found across CRIMZON.

When trying to estimate accumulations of potential losses from cyber, insurance and reinsurance companies face two main challenges: identifying which policies are exposed to the same cyber events and determining how many policies will be affected at the same time. The former is related to the problem of enumerating all technologies and service providers each insured relies upon, the latter is equivalent to estimating the footprint of a cyber event. Analyzing accumulations by CRIMZON enables risk professionals to make sense of the size and extent of potential losses from cyber, without necessarily needing to collect detailed information about technologies and service providers for each insured. The framework is completely agnostic to the line of business, therefore unlocking a full range of possible applications across both silent and affirmative cyber coverages.

Among these applications is the development of aggregate models. This research shows it is possible to estimate the two key ingredients needed for the development of industry loss curves, the hazard and the exposure, using the CRIMZON as the atomic unit of aggregation. By identifying the correlation across CRIMZON, an aggregate model can then be developed.



1. The research group was compiled according to criteria detailed in Appendix A.

Introduction - What are CRIMZON™?

The Cyber Risk Accumulation Zones (CRIMZON™ framework[2] defines the minimal elements needed to provide a view of aggregated cyber exposure. Kovrr launched CRIMZON™ during participation in the fourth cohort of the Lloyd's Lab, the insurance technology accelerator operated by Lloyd's of London. CRIMZON is an open framework created to facilitate better communication across players in the cyber insurance value chain. The framework allows users to overlay their data pertaining to loss, cyber attack frequency, as well as additional data onto the CRIMZON for additional insights of risk per zone and to detect correlations between different zones. The framework was created to support efforts for setting a standard for data collection for cyber exposure management.

The CRIMZON are composed of the following three elements:

- Location - country-level worldwide and state granularity in the US-based on the ISO3166 Alpha-2 standard.
- Industry - an industry classification based on the SIC classification system.
- Entity Size - four commonly used revenue classification bands in the insurance industry.

The framework is built to accommodate various levels of data available. In cases of insufficient data, a data extrapolation technique can be applied for missing data points. CRIMZON can be analyzed with low or high granularity and in various combinations. The views are built to accommodate the ability to use the framework despite varying quality of data within a group of risks.

Background

Kovrr's impact based modeling framework addresses two main event types that can trigger a cyber event. The first event type is service provider events. These events are a failure of a third-party service provider, such as an email provider, cloud provider, etc. Third-party providers are a dominant part of modern IT architecture and are used by many companies operating today. Any damaging event (such as service outage, data leak, data loss for a third-party provider can lead to significant damage that will entail claims from different coverage type (e.g. BI and extra expenses, restoration, regulatory fines).

The second event type is technology events. These are events that are caused by a flaw in a common third-party software library (shared pieces of code between technology providers or a widely used product. An example of this event can be a vulnerability in a commonly used database server or a vulnerability in an encryption software library which is used in multiple products such as web servers, point-of-sale, etc.

2. https://www.kovrr.com/CRIMZON

In Kovrr's whitepaper "Cyber Catastrophes Explained," a cyber catastrophe is defined as "an infrequent cyber event that causes severe loss, injury or property damage to two or more, but typically a large population of cyber exposures." In order for a cyber catastrophe to occur, companies must have a disruption to an important common system or process that is related to either technologies or service providers.[3]

The following three elements were found to have a correlation to technologies and services. Each of the elements are already independently used by the insurance industry for analysis of accumulation and for reporting purposes and therefore most (re)insurers should have access to the data surrounding at least one of the elements.

- Location - due to language and localization, local targeted marketing, trends and culture.
- Industry - companies tend to pick products that answer the specific needs of the business.
- Entity Size - the size of a company usually determines the nature and scale of the product, for example, larger companies require more robust or complex products to handle their data and infrastructure as opposed to smaller companies, and have more resources to invest in solutions.

Pursuant to this observation, this paper highlights a subset of Kovrr's research, which serves as the core empirical validation for the CRIMZON framework. The research, an analysis of the technographics[4] of thousands of companies across five countries, focuses on industries that have suffered cyber attacks in the past and have high cyber insurance purchase rates.[5]

The primary resource utilized in this research is Kovrr's Industry Exposure Database (IED) which holds detailed firmographic data for millions of unique businesses worldwide. The data contains all elements of a CRIMZON: company locations, industry classifications, and estimated revenues.

Research Questions

The research confirms the following hypotheses:

1. **Companies in different CRIMZON tend to use different technologies and service providers.**
2. **Companies within a CRIMZON tend to use the same technology and services.**

3. https://www.kovrr.com/resource/cyber-catastrophes-explained
4. Technographics are the technologies and service providers used by a specific company.
5. More Cyber Insurance Buyers as Awareness Grows, Marsh LLC, 2019

Research Methodology

The initial step of the analysis methodology was to determine research parameters, a study group and a control group.

1. Research Sample Selection Criteria

In this research there was a need for defining selection criteria in order to narrow down the full data set of companies in Kovrr's IED to a representative sample for the study and control groups.

Kovrr's IED dataset was narrowed down by choosing a research and control group based on two criteria: one is the location of the companies (five countries), and the second is the technographics, meaning, choosing two specific categories of technologies and service providers used by companies.

1.1. Location

In order to prove and demonstrate the application of the CRIMZON concept globally, the research focuses on a sample of technologically and industrially developed countries. The countries contain millions of companies spread across different industries and sectors: US, Germany, UK, Japan and Spain. The analysis of a large, yet focused group, shows both the diversity within each country and the differences that arise within a global distribution.

1.2. Technologies and Service Providers

Another criteria is the specific services and technologies in use by companies in the chosen countries. When analyzing, technologies and services, hosting and mail[6] were chosen due to the fact that they are among the most common components of infrastructural operations and directly influence the internet presence of companies worldwide.

Outage or any other type of disruption to these services and technologies (from technical malfunctions to targeted cyber attacks and ransomware could lead to significant business interruption, privacy/security leaks and/or breaches or other issues which would result in reputational damage, lost income, recovery expenses, legal fees, fines and more.

2. Research Study Group

The dataset was composed by extracting all the relevant data of companies in Germany, the US, the UK, Spain and Japan from Kovrr's IED. The companies were then grouped by CRIMZON, amounting to a total of 3,484 CRIMZON. Out of this list of CRIMZON, a study group of 120 CRIMZON was determined by picking CRIMZON with the highest relevance to the cyber insurance market.[7] The total number of unique companies in the study group is 20,000, with the average number of 152 companies within a CRIMZON, and median of 86.

6. Hosting Service - provides accessibility to online websites or services.
Mail Technology and Service - a system for exchanging messages between companies and/or individuals using online services or a locally installed technology.
7. The research group was compiled according to criteria detailed in Appendix A.

3. Control Group

In order to account for the CRIMZON hypothesis, a control group was established to allow for comparisons. The control group consists of the same companies that appear in the 120 CRIMZON picked as the research group, however, instead of being grouped by CRIMZON, they are grouped into 120 clusters following a uniform distribution. These 120 clusters of companies are parallel in size in terms of number of companies to the research group. In other words, a CRIMZON with 300 companies has a corresponding cluster (in the control group) with 300 companies as well (not necessarily the same companies). This was necessary in order to show the influence of the elements on the CRIMZON framework and its potential when assessing exposure and risk.

4. Research Study Sub-Group for Micro Analysis: Industries Relevant to Cyber Insurance

In an effort to provide comprehensible examples from the study group which are particularly relevant to cyber insurance, the original list of 120 CRIMZON was narrowed down to a subset of 35. This sub-group is focused exclusively on industries with high cyber insurance purchase rates in each of the five countries.[8]

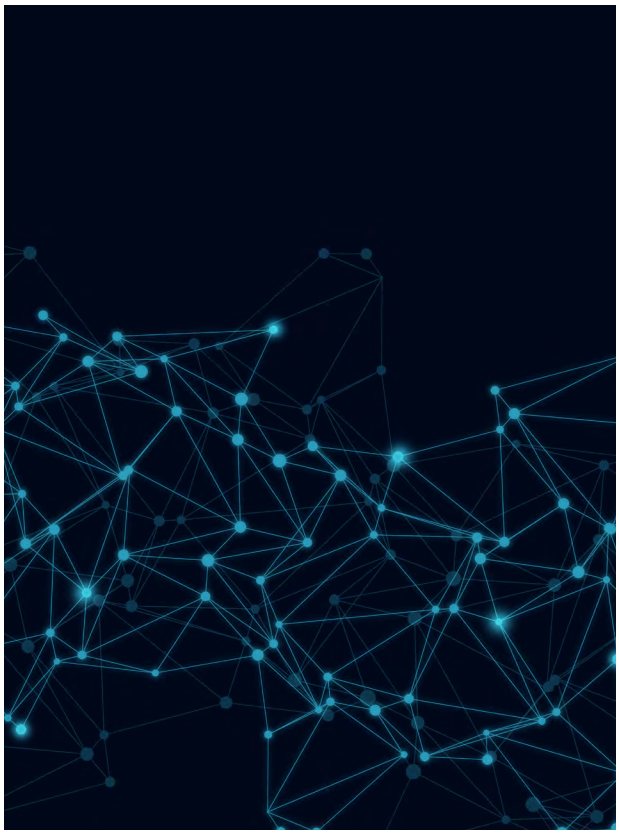
The average number of companies per CRIMZON in this subgroup is 231 with a median of 132. The minimum number of companies within a CRIMZON is 50.

Analysis and Results

The data shows a concentration of same service providers and technologies being used by companies within a CRIMZON. Additionally, the data shows different compositions of service providers and technologies across CRIMZON.

Moreover, the analysis shows concentration of technologies and services when accumulated solely by location, and accumulation is further concentrated, when adding the additional elements of the CRIMZON, entity size and industry to the analysis.

During the analysis process, it was evident that companies can use more than one provider for the same service or more than one technology for the same purpose. Hence the distribution of the service providers and technologies within a CRIMZON presented is the calculation of the number of appearances of the technology or provider in the group (and not by the number of companies using them or their percentage of use within a company.



8. The sub-group was composed of CRIMZON according to criteria detailed in Appendix B.

1. Analysis Across 120 CRIMZON™ and a Subset of 35 CRIMZON™

The heat-maps below present the distribution of mail and hosting service providers and technologies across the subset of 35 CRIMZON of the study group.[9] The X-axis lists the service providers and technologies in a category (mail/hosting) ordered by market share,[10] and the Y-axis are CRIMZON ordered by location.

- It is evident that within the same CRIMZON (each row) there is a concentration of technographics (the colors of the squares describing the level of concentration).
- When comparing CRIMZON, the composition of the technographics (in the same category) is different between the CRIMZON (the colors are distributed differently).

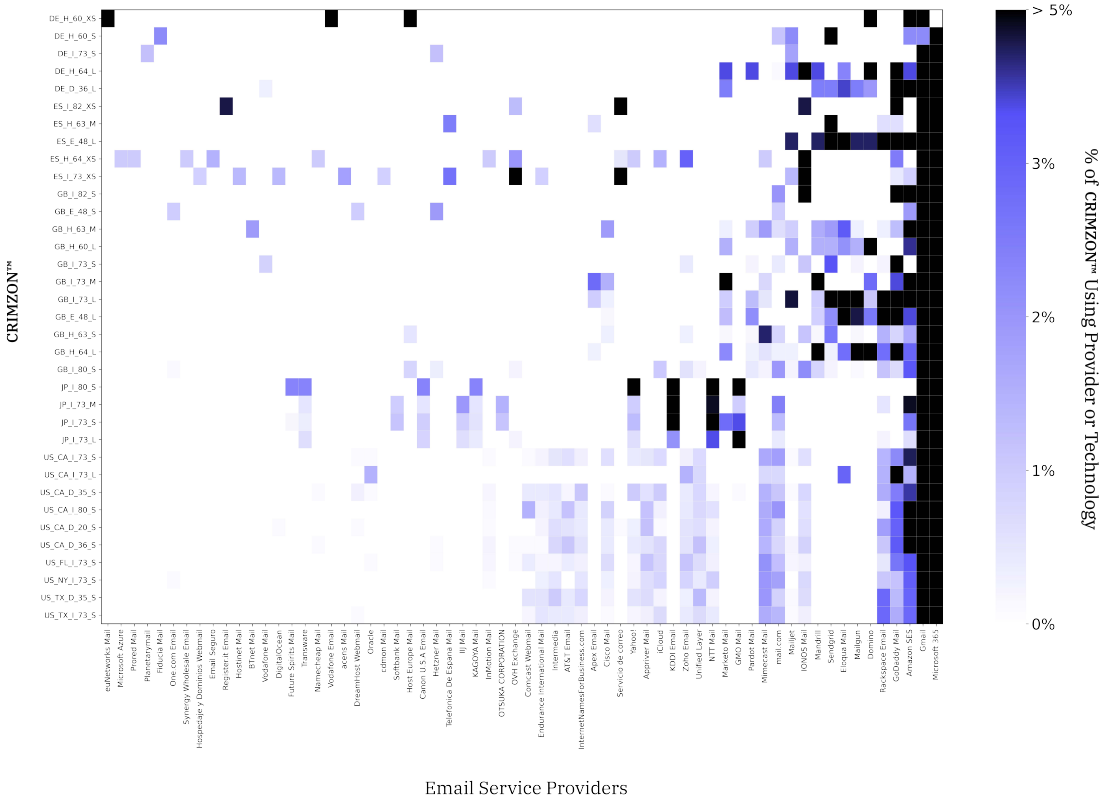


Figure 1: Mail Technologies and Service Providers within a subgroup of 35 CRIMZON by Providers Market Share[11]

9. For heatmaps presenting the distribution of mail and hosting service providers across all 120 CRIMZON please see Appendix C.
10. https://www.datanyze.com/market-share/email-hosting--23
https://www.datanyze.com/market-share/web-hosting--22
11. For the extended heatmaps of representing the study group of 120 CRIMZON, please see Appendix C.

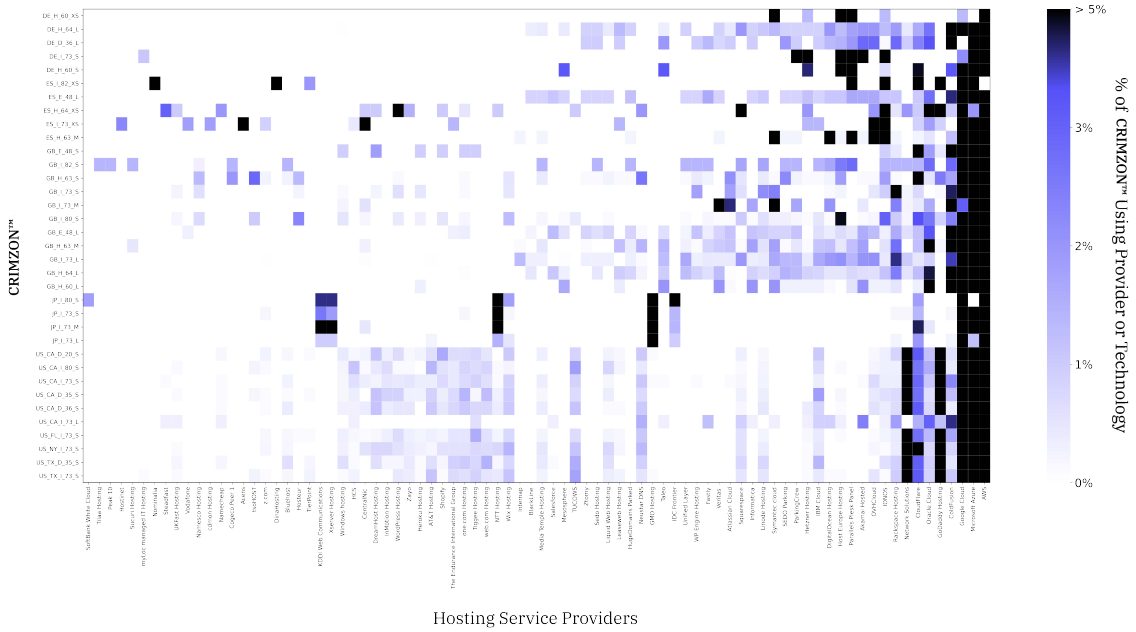


Figure 2: Hosting Technologies and Service Providers within a subgroup of 35 CRIMZON by Providers Market Share[12]

2. Comparison of CRIMZON™ to Control Group

The table below presents a summary of the comparison between the number of distinct service providers and technologies for hosting and mail that are in use in a CRIMZON and in use in its corresponding control group cluster (across all 120).[13]

Number of Distinct Technographics Used by Companies in CRIMZON™ and Control Group Clusters

	Number of Distinct Hosting Technologies and Service Providers		Number of Distinct Mail Technologies and Service Providers	
	CRIMZON	Control Group Clusters	CRIMZON	Control Group Clusters
Average	26.28	57.54	18.66	36.29
Median	22	57	12	31.5
Standard Deviation	16.71	20.89	16.37	19.57

The average number of distinct hosting technographics serving the companies within a CRIMZON is 26.28, while in the control groups the average number is 57.54, with medians of 22 and 57 and a standard deviation of 16.71 and 20.89, respectively. The previous observation shows higher concentration of technographics within CRIMZON than in the control groups, which shows fewer technology and service providers serving the same number of companies.

12. For the extended heatmaps of representing the study group of 120 CRIMZON, please see Appendix C.
13. Determined by counting the total number of distinct providers in a given CRIMZON or control group cluster.

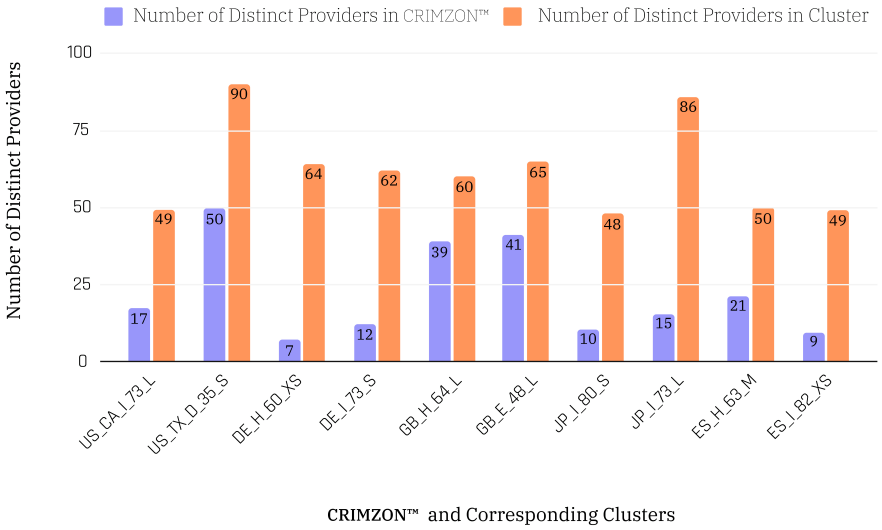


Figure 3: Number of distinct hosting technologies and service providers within a CRIMZON vs. corresponding control group cluster

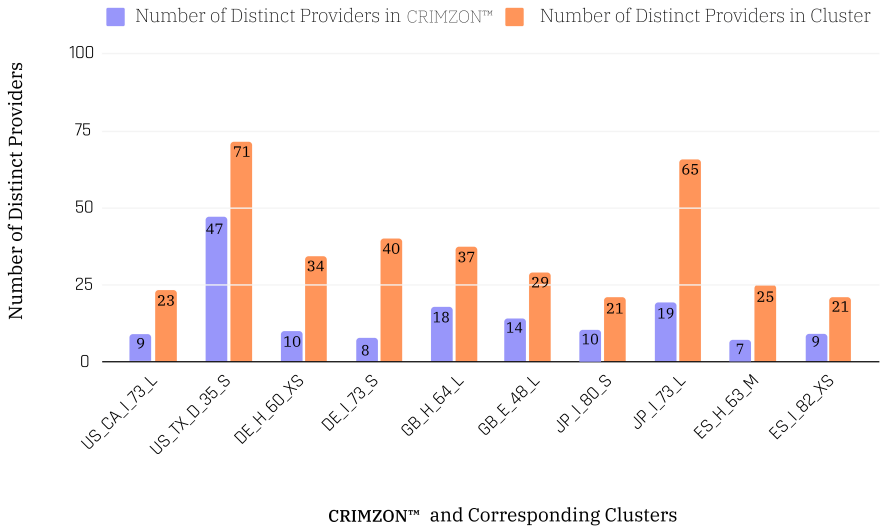


Figure 4: Number of distinct mail technologies and service providers within a CRIMZON vs. corresponding control group cluster

Visible in Figures 3 and 4, the total number of distinct services providers and technologies in the CRIMZON is always lower than in the control group cluster. A statistical significance test shows that the results are extremely unlikely to be the result of random chance ($p < 0.0005$).

3. Detailed Examples of Top Technographics (Comparison between CRIMZON and Control Groups)

The table below shows the top three hosting and email technologies and service providers in several of the CRIMZON in the research group and in their corresponding clusters in the control group.

		Top 3 Hosting Technologies and Service Providers	Top 3 Mail Technologies and Service Providers
Example no. 1	US_CA_I_73_L California, US Business Services Large	AWS Google Cloud Microsoft Azure	Gmail Microsoft 365 GoDaddy Mail
	Corresponding Control Group Cluster	AWS Microsoft Azure Google Cloud	Gmail Microsoft 365 Rackspace Email
Example no. 2	DE_H_60_XS Germany Depository Institutions Extra small	Host Europe Hosting Parallels Plesk Panel Symantec Cloud	Domino Amazon SES Host Europe Mail
	Corresponding Control Group Cluster	AWS Microsoft Azure Google Cloud	Microsoft 365 Gmail Amazon SES
Example no. 3	GB_E_48_L United Kingdom Communication Large	AWS Microsoft Azure Google Cloud	Gmail Microsoft 365 GoDaddy Mail
	Corresponding Control Group Cluster	AWS Microsoft Azure Google Cloud	Microsoft 365 Gmail GoDaddy Mail
Example no. 4	JP_I_80_S Japan Health Services Small	Google Cloud GMO Hosting AWS	Gmail NTT Mail GMO Mail
	Corresponding Control Group Cluster	AWS Google Cloud Microsoft Azure	Microsoft 365 Gmail GoDaddy Mail
Example no. 5	ES_I_82_XS Spain Educational Services Extra small	Parallels Plesk Panel Google Cloud IONOS	GoDaddy Mail Gmail IONOS Mail
	Corresponding Control Group Cluster	AWS Microsoft Azure Google Cloud	Gmail Microsoft 365 Rackspace Email

The top three providers in the control group clusters are composed of the leading technographics in the global market, for example, Google or Amazon. The top three providers in the CRIMZON are likely to include a local or regional provider as well. This can be observed in CRIMZON: JP_I_80_S (small companies in the healthcare industry located in Japan) where two out of the top three email providers for the entire CRIMZON are local Japanese companies. Additionally, this occurrence is also reflected in CRIMZON ES_I_82_XS (extra small companies in the education industry located in Spain) where 2 out of the 3 top hosting providers are European. The presence of local providers can be further seen in Figure 1, where there is a large concentration of Japanese providers - NTT, GMO and KDDI only in CRIMZON in Japan. No CRIMZON outside of Japan in the sample uses these providers.

4. The Location Element and its Contribution to Risk Accumulation in Cyber

Location is often dismissed in cyber risk assessment because the effects of technology events can be global. While location is often assumed as an unimportant factor for aggregating loss in cyber, compared to its importance in natural catastrophe modeling, this research shows that location plays a role in contributing to cyber risk accumulation.

The table below presents a summary of the comparison between the number of distinct service providers and technologies for hosting and mail that are in use by groups, grouped by only location, compared to their corresponding control group clusters.[14] This analysis has been conducted on the same companies in the research study group (120 CRIMZON).

Number of Distinct Technographics Used by Companies in Location Groups and Control Group Clusters

	Number of Distinct Hosting Technologies and Service Providers		Number of Distinct Mail Technologies and Service Providers	
	Location Groups	Control Group Clusters	Location Groups	Control Group Clusters
Average	74.62	116.5	85.25	144.29
Median	76	113.5	81	137
Standard Deviation	21.79	9.22	41.39	36.32

14. Determined by counting the total number of distinct providers in a given location or control group cluster.

The average number of distinct hosting technographics serving the companies within a group accumulated by location alone is 74.62, while in the control groups the average number is 116.5, with medians of 76 and 113.5 and standard deviation of 21.79 and 9.22, respectively. This observation shows higher concentration of technographics within the groups grouped by location compared to the control groups, meaning fewer technology and service providers serving the same number of companies.

Also, in order to fully illustrate the importance and contribution of the location element in the CRIMZON framework, the distribution of the technologies and service providers has been analyzed while holding the size of the company and its industry constant.

The first step was analyzing the distribution of technographics across all the chosen location zones.
As presented below, when holding the industry and size as a constant, results showed different compositions of technographics used in different locations. This result was observed as statistically valid. [15]

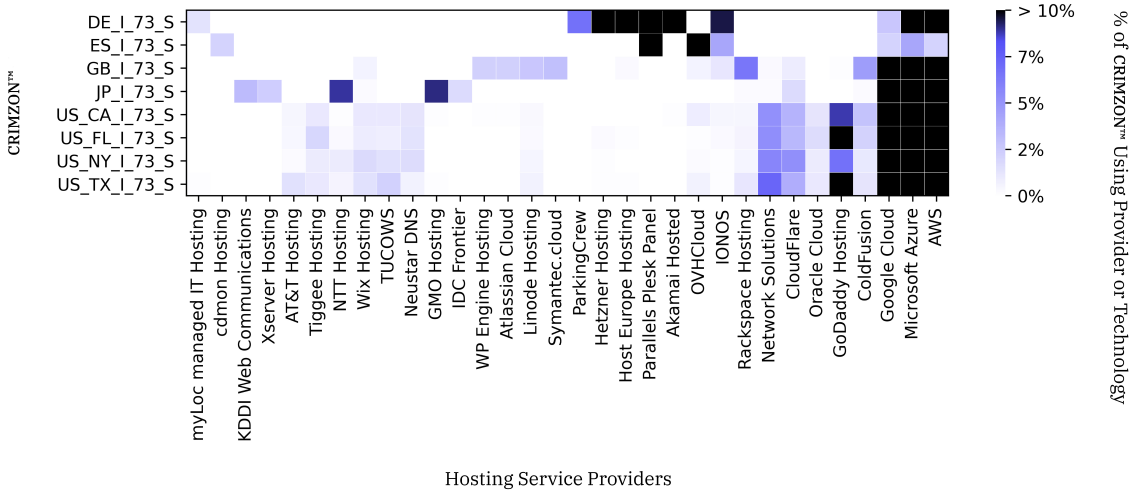


Figure 5: The distribution of hosting service providers and technologies in CRIMZON that differ in their location ordered by providers market share

15. The results of the statistical significance test are $p < 0.005$.

Moreover, when analyzing the distribution of technographics by grouping by location alone (meaning, a variety of industries and sizes appear within the clusters), there is less concentration.

This analysis shows that the element of location within a CRIMZON has an impact on the accumulation of the hazard, and although location has a value for the accumulation of technographics, the industry and size elements add an additional level of insight.

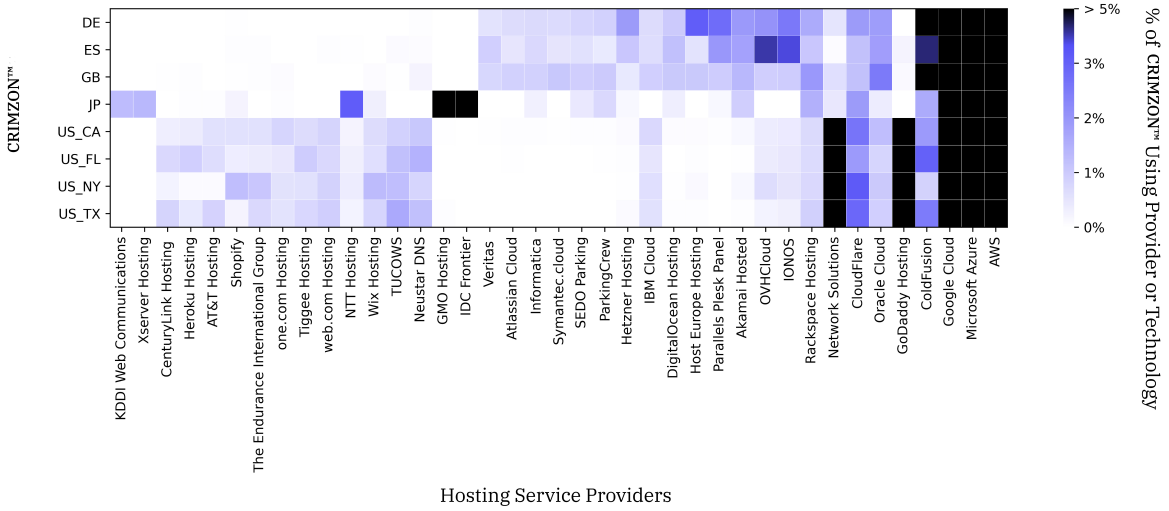


Figure 6: The distribution of hosting service providers and technologies in companies grouped by location alone and ordered by the technographic's market share.

Each of the three elements of a CRIMZON are a contributing factor for more accurate analysis of accumulation (with higher concentration, or less distributed technographics), than by analysis of aggregation of each element separately.

Conclusion

The CRIMZON framework has been developed to enable the insurance market to better segment their cyber risk accumulation. Results of the analysis showed a concentration of technologies and service providers when grouping by location, and further concentration when adding the additional elements of the CRIMZON, entity size and industry to the analysis. These results are a clear indication that companies within the same CRIMZON have the tendency to use the same service providers and technologies, and different CRIMZON contain different compositions of service providers and technologies.

Accurate accumulation of cyber risk based on the hazard can be a cornerstone of addressing some of the main challenges the (reinsurance industry currently faces in the realm of cyber risk modeling. By taking into account location, industry and entity size, the CRIMZON open framework allows users to estimate which type of cyber events are likely to affect their portfolio, without having to have access to extensive technographic data. Importantly, when an event occurs, the CRIMZON framework enables reinsurers and insurers the capability to estimate how the event may spread across CRIMZON and apply this knowledge to understand the impact on a portfolio.

The footprint of a cyber catastrophe is described mainly by two parameters: the technology or service provider involved and the propagation pattern of the infection. The resulting trail of damage can also be described more simply by listing the CRIMZON affected. This observation naturally leads to two possible developments for the framework: event response capabilities and correlation across CRIMZON. The latter is currently a key consideration taken into account in Kovrr's catastrophe model framework. The ability to overlay details of an unfolding event would enable insurance companies to react accordingly, respond more efficiently and ultimately better serve their clients.

Ultimately the concept of CRIMZON is a natural candidate to become the atomic unit of aggregation for an industry loss model for cyber. This research shows it is possible to estimate the two key components for the development of industry loss curves by CRIMZON: the hazard and the exposure. By estimating the correlation across CRIMZON, an aggregate model can then be developed.

Appendix A

Research Group Composition (120 CRIMZON™)

1. Location

USA | Germany | UK | Spain | Japan

2. Industry

Mining **(B)**

- **13** - Oil And Gas Extraction

Construction **(C)**

- **17** - Construction Special Trade Contractors

Manufacturing **(D)**

- **20** - Food And Kindred Products
- **22** - Textile Mill Products
- **24** - Lumber And Wood Products, Except Furniture
- **27** - Printing, Publishing, And Allied Industries
- **28** - Chemicals And Allied Products
- **35** - Industrial And Commercial Machinery And Computer Equipment
- **36** - Electronic And Other Electrical Equipment
- **37** - Transportation Equipment
- **39** - Miscellaneous Manufacturing Industries

Transportation, Communications, Electric, Gas, And Sanitary Services **(E)**

- **48** - Communications
- **49** - Electric, Gas, And Sanitary Services

Wholesale Trade **(F)**

- **50** - Wholesale trade durable
- **51** - Wholesale trade non-durable

Retail Trade **(G)**

- **55** - Automotive Dealers And Gasoline Service Stations
- **56** - Apparel And Accessory Stores
- **59** - Miscellaneous Retail

Finance, Insurance, And Real Estate **(H)**

- **60** - Depository Institutions
- **62** - Security And Commodity Brokers, Dealers, Exchanges, And Services
- **63** - Insurance carriers
- **64** - Insurance Agents, Brokers, And Service
- **65** - Real Estate
- **67** - Holding And Other Investment Office

Services **(I)**

- **70** - Hotels, Rooming Houses, Camps, And Other Lodging Places
- **73** - Business Services
- **80** - Healthcare
- **81** - Legal Services

82 - Educational Services
83 - Social Services
86 - Membership Organizations
87 - Engineering, Accounting, Research, Management
89 - Miscellaneous Services

3. Size

Micro **(XS)**: Annual revenue less than $10M
Small **(S)**: Annual revenue $10M-$250M
Medium **(M)**: Annual revenue $250M-$1B
Large **(L)**: Annual revenue greater than $1

Appendix B
Research Group Composition (35 CRIMZON™)

1. Location

USA | Germany | UK | Spain | Japan

2. Industry

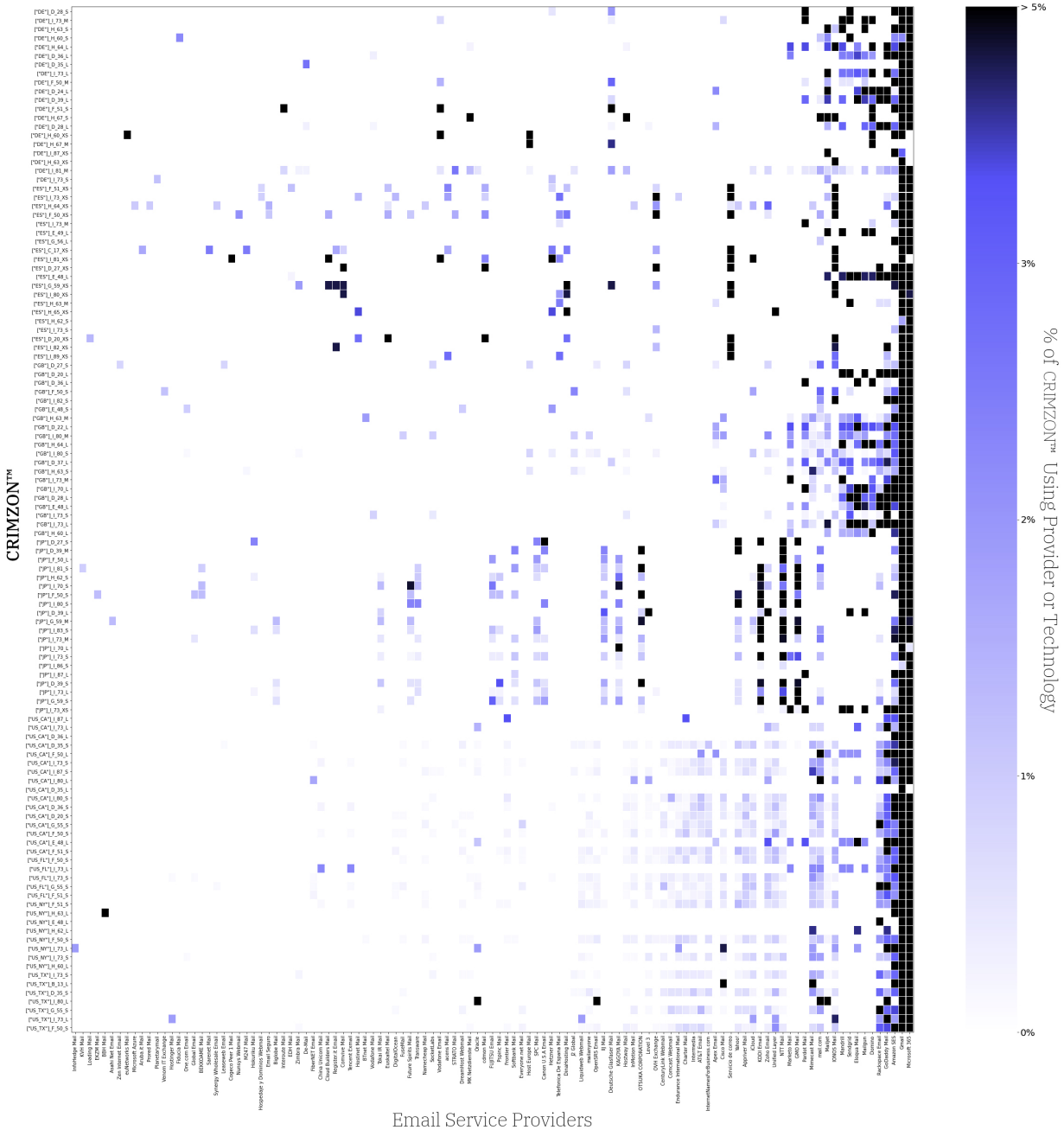
Mining **(B)**
13 - Oil And Gas Extraction
Manufacturing **(D)**
20 - Food And Kindred Products
35 - Industrial And Commercial Machinery And Computer Equipment
36 - Electronic And Other Electrical Equipment
Transportation, Communications, Electric, Gas, And Sanitary Services **(E)**
48 - Communications
Finance, Insurance, And Real Estate **(H)**
60 - Depository Institutions
63 - Insurance carriers
64 - Insurance Agents, Brokers, And Service
Services **(I)**
73 - Business Services
80 - Healthcare
82 - Educational Services

3. Size

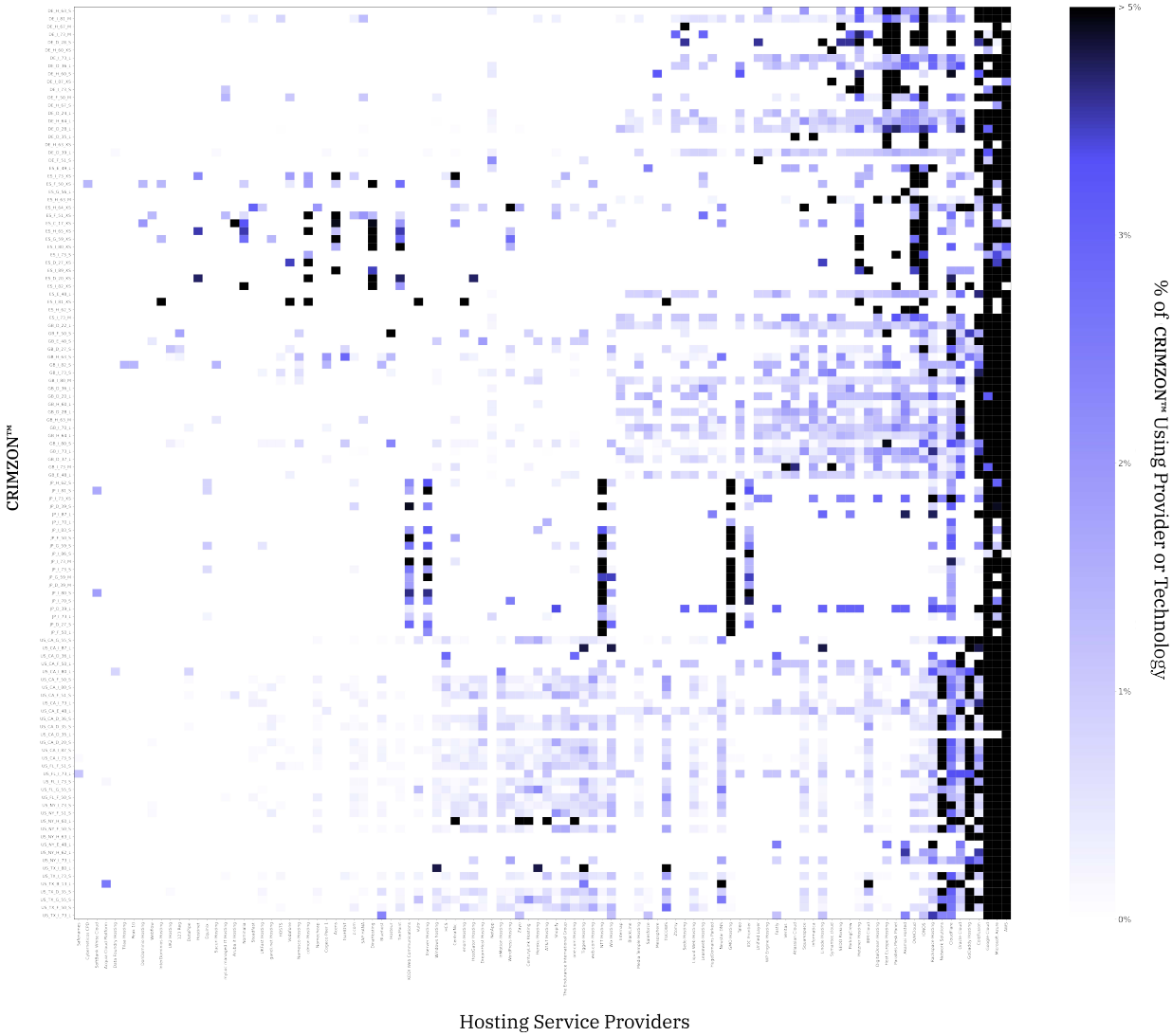
Small **(S)**: Annual revenue $10M-$250M
Large **(L)**: Annual revenue greater than $1B

Appendix C

Extended Heatmaps of Technologies and Service Providers Across 120 CRIMZON™



Mail Technologies and Service Providers within 120 CRIMZON by Providers Market Share



Hosting Technologies and Service Providers
within 120 CRIMZON by Providers Market Share

The Authors

Marco Lo Giudice, PhD

Head of Pricing Models Development

Or Amir

Product Manager

Geniya Brass Gershovich

Cyber Intelligence Analyst

Amos Israel

Risk Data Scientist

Contributors

John Butler, David Clouston, Visesh Gosrani and Naomi Weisz also contributed to this report.

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers transparent, real-time data- driven insights into their affirmative and non-affirmative cyber risk exposures. The Kovrr platform is designed to help underwriters, exposure managers and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.

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