KOVRR
Cyber Risk Modeling

www.kovrr.com

Using CRIMZON™ to assess cybersecurity hazards with an insurance portfolio

OCTOBER 2021

In recent years, the rise to prominence of cyber risk, both as a peril and as a line of business, has created opportunities and threats to insurance companies in equal measure. Insurance executives, exposure managers and underwriters need now more than ever to understand, quantify and manage their exposures, in order to sustain profitability and to protect their balance sheets.

By definition, cyber events occur due to vulnerable technology. It is therefore tempting to conclude that understanding these exposures requires knowing the full map of technologies and service providers an insured relies upon, including the granular details on how data is stored and accessed. The issue with this approach is that while this information is certainly valuable to assess the risk, it is challenging to obtain at scale due to the difficulties that arise from accessing and analyzing the data properly.

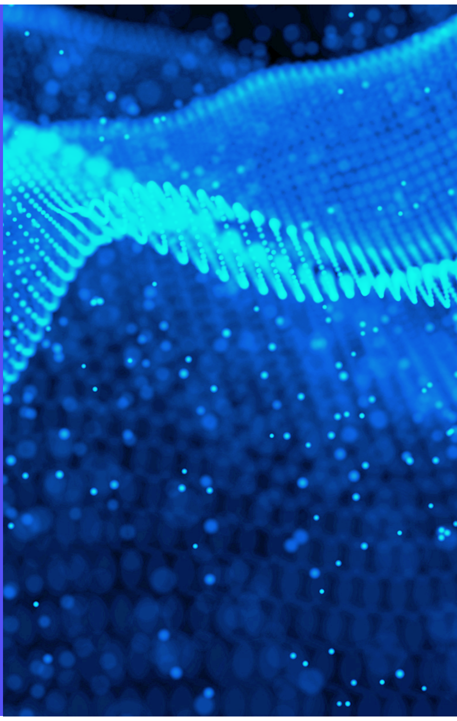
Help in solving this dilemma is provided by using techniques to analyze the cyber footprint of an insured, mapping the technologies and service providers most exposed to the external world. The premise being that such analysis provides insurers with the same point of view of potential threat actors. It is fair to say this is currently the gold standard of cyber hazard analysis. Insurance carriers with large affirmative cyber books rely on external scans for underwriting as well as for portfolio management, often augmenting this data with information provided by the insured, mostly from third-party vendors.

A direct relationship with the insured is the best way forward to understand their level of risk, however, it’s disingenuous to assume every stakeholder in the insurance industry is able to access the same level of data. Within the same company, portfolio managers often don’t have access to the same level of details as underwriters, and across entities reinsurers rely on their clients passing on data, which requires overcoming hurdles around data confidentiality as well as technical limitations on data volumes. Moreover, external scans are expensive and might not be a viable option when cyber coverage is offered as an endorsement on other lines of business.

Assessing hazard insured by insured is therefore not always possible and cannot be expected to be the only way. Kovrr has developed an open framework, CRIMZON, which allows insurance stakeholders to understand hazard without running expensive analysis tools and collecting only a minimum amount of data points. This framework is designed to answer basic questions on cyber risk accumulations and estimates of Probable Maximum Loss (PML). It allows full flexibility around the type of risk analyzed, whether the focus is ransomware or cyber liability, and is consistent and compatible with the catastrophe model methodology deployed in our probabilistic quantification solution.

Mr. Hetul Patel, Advisor to Kovrr and Chief Actuary at Liberty Mutual Re said:

> “CRIMZON™ are a novel way to address the very real need for better cyber risk aggregation. Recent events have clearly highlighted that cyber loss events can’t be managed through the traditional tools that reinsurers currently use. CRIMZON have the potential to create a market standard, similar to the way cresta zones are used for natural catastrophe modelling. The use of which goes beyond aggregate and risk management, and into outward reinsurance purchasing and attracting third party capital.”



Grouping Companies Together by CRIMZON™

Kovrr's open framework Cyber Risk Accumulation Zones (CRIMZON) groups companies together based on three characteristics: industry, location and entity size. This framework for grouping is based on research that shows that companies sharing these characteristics tend to share cyber risks. Cyber attacks would then be more likely to spread through companies within the same CRIMZON rather than hitting companies randomly.

For example, a cyber attack might be targeted at large healthcare organizations in the U.S., meaning companies that fall into this CRIMZON (based on industry, location and size) could be at risk. Yet companies in another CRIMZON, such as small technology companies in Japan, might not be at a high risk for that same attack.

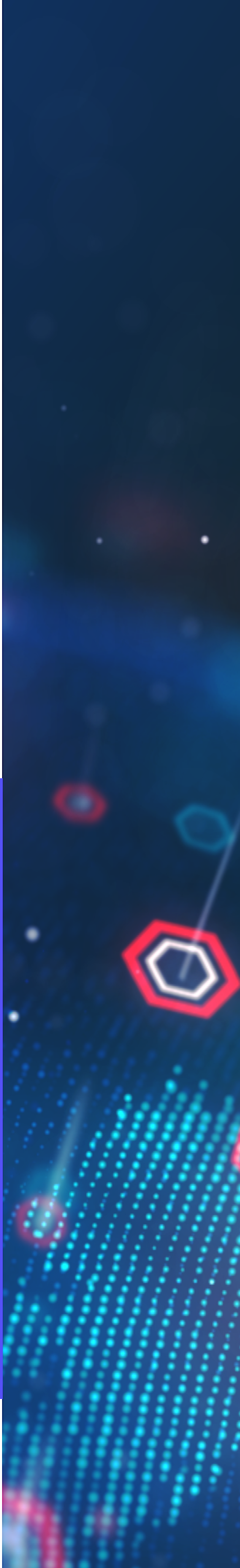
More specifically, companies within the same CRIMZON tend to face the same risks because they use similar technologies and service providers. An attack on one vendor could ultimately affect most companies across a CRIMZON who use the same vendor.

Grouping companies within an insurance portfolio into different CRIMZON thus helps to aggregate maximum exposure. Users can see how much of a portfolio is at risk for a given event, similar to how insurers aggregate exposure for natural disasters within geographic zones.

Additionally, it's possible to dive deeper than just aggregate exposure. Insurers can delve into specific risks companies within particular CRIMZON face. But how? By looking at the specific technologies and service providers that these companies tend to share. CRIMZON provide a general bucket, but it's possible to then look at the general categories of technologies and service providers, such as email providers, and see which vendors in particular a company is likely to use based on their location, industry and size.

Mr. Tom Quy, Senior Vice President- Acrisure Re said:

> "CRIMZON™ are a concept that contributes to the further understanding and development of the cyber insurance market. The availability and expansion of reinsurance capacity is likely to be predicated on a greater understanding of the potential for concentrations of risk through aggregation areas including software and service providers. This framework enables (re) insurers to group risk exposures and also to minimize and mitigate build-ups of concentrations of exposures to cyber risk. CRIMZON allow insight into key aspects regarding reinsurance purchases, such as average losses relative to tail events and average industry exposure per zone. CRIMZON are therefore useful for both portfolio diversification and reinsurance purchasing decisions. We expect that this will increase the maturity of the conversations we have with insurers about the type of reinsurance that is suitable for them and thus increase the value they both perceive and achieve from their reinsurance"



Analyzing Cyber Security Hazard

Given the vendor commonalities among companies within the same CRIMZON, Kovrr defines cybersecurity hazard as the enumeration of the technologies and service providers that a company relies upon for business.

From there, it's important to clarify what a cyber event means, which Kovrr defines as: a disruption for a service provider for a certain amount of time or an exploitation in a technology causing a malfunction in a technology.

With this definition, it's important to be able to enumerate the technologies and service providers that the companies use. While this enumeration may seem like an impossible task, the reality is that the real risk lies in the assets reachable from the outside, i.e., connected to the internet. That means companies can be analyzed from the outside.

A Priori Process

To analyze companies' technologies and service providers, Kovrr starts by running an external scan to look at everything that is exposed via the internet. For example, if a website accepts payments where customers can enter credit card details and related information, this can be defined as a source of exposure. Scanning millions of companies across the globe, and keeping a record of what technologies and service providers they use, allows for finding specific commonalities.

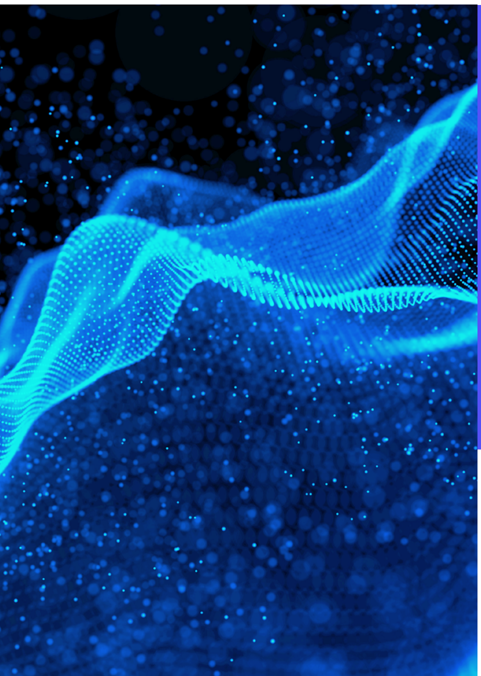
Doing the work of running these scans, rather than making assumptions such as guessing that all large manufacturers use the same type of operating system, allows for finding peculiarities in specific markets. It also allows for defining "known unknowns." It may not be possible to determine every hazard, but it's useful to at least see which areas can be assessed a priori and which areas lack information to make any meaningful analysis.

If hazard within a portfolio is properly defined, (re)insurers can dive deeper into modeling risk based on the data pertaining to analysis of a company's general exposure.

By acquiring third-party, macro-level data on technologies and service provider usage, Kovrr makes educated assumptions on technologies being used within specific CRIMZON and can therefore model a company's exposure accordingly. Additionally, if specific data does not surface in an external scan, yet it shows up in the macro-level data, that scan shows that there may be a security gap that needs to be addressed. For example, scans might show that manufacturers of a given size and geography tend to use the same types of controls for their machines. If those controls do not show up for one manufacturer being scanned, that could be an indication of a gap.

Conversely, a technology that's only used by a handful of manufacturers and doesn't show up in one scan wouldn't likely indicate a gap. Retailers might depend upon a portal to sell their goods, and suppose that shows up in most scans. The same type of portal then shows up in a few scans for manufacturers who have a small retail operation, but it's not part of their core business. Therefore, if a scan for another manufacturer doesn't show that portal, it can reasonably be assumed that even if that company uses that specific technology, it does not pose significant cyber risk, as it's not core to company operations.

In other words, by analyzing millions of companies, Kovrr can find commonalities and determine what types of technologies and service providers tend to be used by certain companies and therefore pose a risk.



Ms. Timea Töröcsik, Head of Global Financial Lines Portfolio Management & Pricing bei Allianz Global Corporate & Specialty (AGCS) said:

> "CRIMZON™ are valuable indicators and enablers of further development of the cyber insurance market. Using the CRIMZON allows us to get better portfolio segmentation and be able to focus our attention on significant exposure areas. In addition, we really appreciate the detailed analysis KOVRR is doing on each zone."

Comparing Cyber Hazard to Natural Hazard

Cyber hazard modeling can be compared to natural hazard modeling. For example, when looking at hurricane risk, there are certain clearly defined parameters, like distance to the coast. The further inland a property is, the less likely it generally is to be at risk from a hurricane, considering that hurricanes start to dissipate as they make landfall. So assessing a property's location allows for the general assessment of risk. There will be variances based on factors unique to specific properties, like elevation and construction material, but it's possible to assess a portfolio of properties, based on the average risk for a property in a given zip code.

> The same concept applies with modeling risk for cyber hazards, just with different perils. By scanning as many companies as possible, Kovrr can assess, on average, what technologies and service providers a company uses and how that, on average, translates into loss exposure.

Benefits for Reinsurers

Assessing cybersecurity hazard through these types of scans not only helps insurance carriers gauge their exposure. It also can be beneficial for reinsurers. In many cases, an insurance company buying reinsurance would not dive into as much detail regarding the risk of specific companies within their portfolio. One reason for this is that even if an insurer shares everything about their book when purchasing reinsurance, that book may look completely different in a year, because it's always changing.

Still, reinsurers need to evaluate the risk that's inherent in an insurance carrier's portfolio, meaning they need to be able to say something about what technologies and service providers are commonly used in the portfolio to then understand the biggest sources of accumulation. In this case, a reinsurer can leverage Kovrr's industry exposure database, compiled of millions of scanned companies, to understand the average composition of technologies and service providers in a specific portfolio.

Conclusion

The CRIMZON framework allows insurance carriers to gain some insights into the hazard of cyber without necessarily needing to run external scans or in the absence of a direct relationship with the insured. It also allows for efficient data exchange with reinsurance and other capital providers. All stakeholders in the chain have access to the same indication of risk, from hazard to exposure accumulations.

This basic level of understanding enables the identification of risk accumulations at a glance, providing a language for communicating these findings at all levels. The vast amount of data required to understand the risk is distilled in simple blocks defined by three dimensions: industry, geography and size. The concise nature of the CRIMZON framework, coupled with the power of a cyber probabilistic model, is currently helping some of the most sophisticated insurance and reinsurance companies manage and communicate their risk.

All this is possible because businesses within the same CRIMZON not only have the same operational needs for technology and service providers, but also tend to limit their choices of products to a selected few. Understanding the hazard for cyber risk is therefore equivalent to understanding these choices.

The Author

Marco Lo Giudice, PhD

Head of Pricing Models Development at Kovrr

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals 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