AXIS INCYTE London 2018
Quantifying Cyber Risk Panel Notes

AXIS Cyber Insurance Centre of Excellence launch event - INCYTE 2018 – Quantifying Cyber Risk - Panel Debate

A panel conversation designed to give the audience an objective view into the world of cyber risk quantification. Cyber risk quantification receives a lot of criticism. The CoE wanted to provide our guests with a view of; how it is currently being done, the things preventing the industry from doing it better and what could be done to improve it. Hopefully, dispelling some myths, and building trust and confidence in insurance and cyber products generally.

What is the definition of cyber risk within the context of the current cyber risk quantification landscape?

It can be defined as the probability of loss or damage to an asset stemming from a cyber-based threat.

However, there is an issue, most tools and platforms are currently only geared to quantify risks to tangible assets. So what? Intangible assets like IP and reputation are becoming increasingly larger constituents of a company's total value and users of these tools run the risk of limiting their view of the risk landscape and failing to keep pace with customers' needs.

So, in the current context Cyber Risk relates to tangible assets but we must not ignore the need to better understand and quantify the risks intangible assets.

How do companies currently quantify cyber risk?

Typically, they use a combination of empirical data from historic events and other relevant data that they find to be correlated with incidents and counterfactuals and expert judgement to model where there is less information available. This is presented in dashboards as a 'risk score' which is often able to be interrogated further to derive more insights or, provide specific scores for different aspects of the risk.

What data sources are currently used in the quantification of cyber risk?

Platforms like Cyence will consider hundreds of data sources including information around external sentiment like; news media, dark web and social media, internal sentiment such as job postings and job reviews, technical information such as network information, malicious hosts, presence of CDNs, shared hosting, profile information such as industry sector, number of employees, number of locations, record count and many others.

The principle of Garbage In / Garbage Out (GIGO) is a challenge for anyone working in the data analytics space. What process do companies go through to assess the veracity of these data sets initially and on an ongoing basis?

Due diligence processes typically involve assessing both the volume and velocity of the data but just as importantly, uncertainty and precision 'measures' need to be assessed. Most reputable companies will be doing this initially and then periodically as part of their source 'audits', these audits would also be looking to test and validate any assumptions that have been applied to the scoring or weighting of these data sources.

What barriers do we face to getting accurate cyber risk quantification?

There are a number of key barriers.

There is a propensity to focus on how risk relates to the now and not the future despite the technological landscape moving on. We are still doing it this way because it is how we have always done it. Current thinking takes a very 2 dimensional approach and achieves the 3rd dimension (frequency) simply by iteration.

There are gaps in our models and we need access to new data sources. For example, we need to understand; control performance, dependencies (and therefore risk propagation and influence), breadth of harm and harm's true impact on identified risks.

The changing nature of the threat intelligence picture. This is not necessarily a barrier but it is a critical component of the risk quantification equation that is often ignored or not given the focus it needs.

There is little collaboration in the risk quantification space. Contrary to popular belief there is a lot of data out there but companies and organizations do not want to share it.

There is a lack of standardization in the risk quantification space. This makes the processing (Extraction / Transformation / Loading) and analysis of any data challenging.

You need transparency in the assumptions and approaches so as to ensure any systems or partnerships built to take advantage of data sharing are based on sound and logical assumptions.

The pace of change or technology and the impact it will have on the performance of risk controls.

Looking to the future how could we improve the way we quantify cyber risk?

Simply put, it is to address the barriers identified above.

Additionally, where we believe accurate data is essential for quantifying cyber risk, we need to define this data set as pre-competitive (beneficial to all), work as a practitioner community to standardize it, collect it and share this crucial dataset.

Sharing data so it can be scrutinized properly, and that the models are published so the assumptions they make can also be peer-reviewed.

Applying Threat Intelligence to these models to help us predict the range of residual risk we may be exposed to more precisely.

Improve the precision around uncertainty i.e. which components are empirically driven, which ones are driven by assumptions, and how can we think about these different assumptions

What could others be doing to help improve our ability to quantify cyber risk (e.g. government, vendors, insurers, regulators)?

We need regulators to work with the new insights to make sure that regulatory and compliance regimes are incentivizing the behaviors and practice (standardization and information sharing) that truly results in lower residual risks both within a single enterprise AND across sectors.

We need enterprises to get involved. We need them to help collect data possibly becoming living labs that would provide immediate feedback on risk control performance.