DENEXUS

Standards in Quantified Industrial Cyber Risk #2

DeNexus Knowledge Center
Part 1 – The Data Difference

Today, our series continues with DeNexus' Head of Research & Modelling Strategies, Romy Rodriguez Ravines and our Sr Director of Cybersecurity, Juan Carlos Cortinas Abad, presenting the **DeNexus Knowledge Center**, the 'brain' of the **DeRISK Platform** that represents the ***Second Generation in Cyber Risk Quantification and Management.***

In the initial launch of the DeNexus 'Standards in Quantifying Industrial Cyber Risk' series, our CEO Jose Seara discussed Industrial Cyber Risk Trends and Solutions facing industrial asset owners, and the cyber risk transfer industry.

Today, our series continues with DeNexus' Head of Research & Modelling Strategies, Romy Rodriguez Ravines and our Sr Director of Cybersecurity, Juan Carlos Cortinas Abad, presenting the **DeNexus Knowledge Center**, the 'brain' of the **DeRISK Platform** that represents the ***Second Generation in Cyber Risk Quantification and Management.***

We are dividing this paper in two parts: Part 1- The Data Difference and Part 2 – Driving Value from the Data (to be released in our next edition).

DeRISK. An Overview

Let's start with a quick recap, DeRISK is a cloud-based, second-generation leader in cyber risk modeling that is setting the stage as the global standard for industrial cyber risk quantification and management (CRQM) in the Industrial OT/ICS space.

Today's cyber landscape requires an entirely new set of solutions. Increased threats, higher probability of cyber-attacks, new regulatory requirements, potential fines for non-compliance and insurers no longer underwriting against the current attack landscape has left a huge gap in cyber-risk for OT Industrials and Insurers.

DeNexus is bridging that gap! For the first time, industrial asset owners, (re) insurers and ILS funds are provided with evidence-based, data-driven, real-time visibility into their asset's actual cyber risk exposure using data from INSIDE the client's OT network. This Inside-Data enables detailed, bottom-up, portfolio-level cyber risk modeling that the Industrial industry has been missing... until now!

An Introduction to our Knowledge Center

The *DeNexus Knowledge Center* is where DeRISK data, insights and intelligence reside. *DeNexus Knowledge Center* hosts and leverages the critical asset data from inside the client OT network (Inside-Data) together with a global consortium of public, private and proprietary threat intelligence, cyber-breach and loss data (Outside-Data**)** to provide industrial stakeholders with the most ***credible*** and ***accurate*** view of their industrial asset's cyber risk posture.

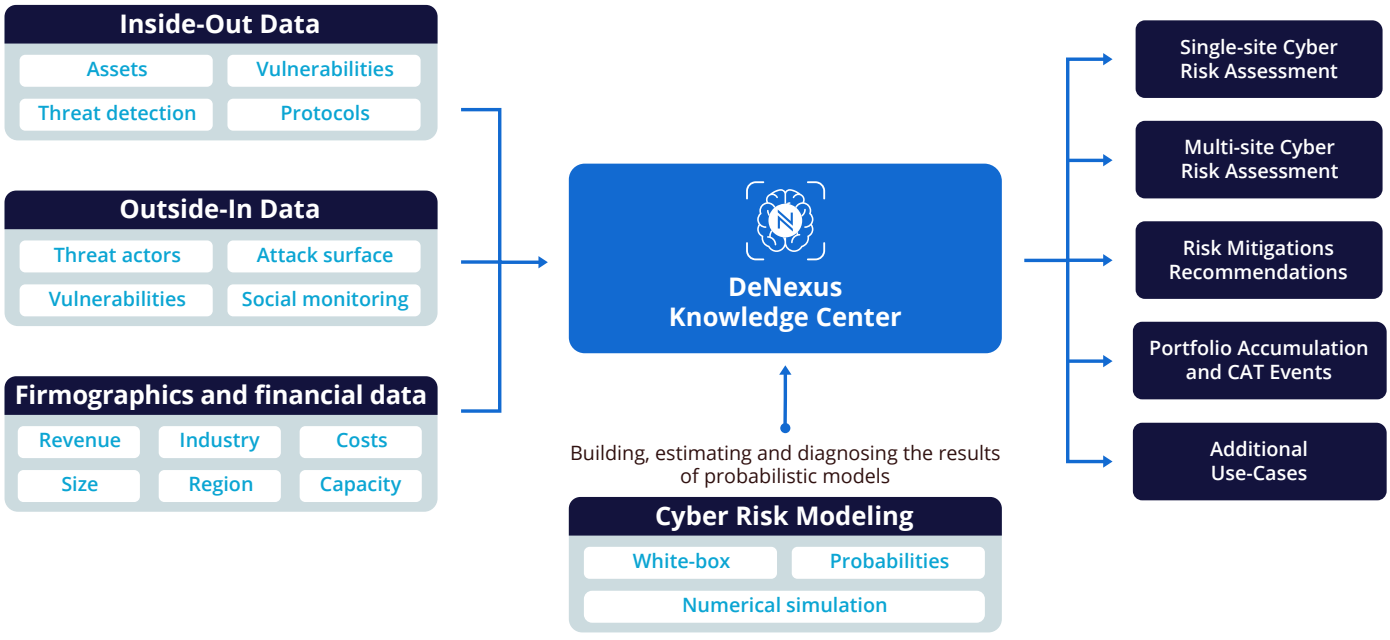
The DeNexus Knowledge Center is where DeRISK data, insights and intelligence reside.

The DeNexus Knowledge Center contextualizes all that Inside-Data and Outside-Data while keeping critical asset information safe, secure, and compliant with the most stringent regulations, thanks to the ***DeNexus Trusted Ecosystem*** which uses a combination of data integrity, encryption and anonymization tools, security standards and certifications, trusted and certified infrastructure, policies and procedures to enable strict control over the storage and the dissemination of cyber data *(more on our Trusted Ecosystem coming soon in the series)*.

Moreover, DeNexus is trending towards having evidence-based inside-data from 10% of the operating assets in the renewable power generation space in the US (a $350 billion industry), and expanding to other industry verticals and geographies, DeNexus Knowledge Center is the knowledge base where the indicators and cyber risk insights reside. Industry benchmarks, enriched data, peer comparison, portfolios and risk accumulation analysis, definition and impact of mitigation projects, validation and calibration of modeling systems, trends of cyber threat and losses are just a few of the use cases unlocked by the DeNexus Knowledge Center.

DeNexus is trending towards having evidence-based inside-data from 10% of the operating assets in the renewable power generation space in the US

For more interesting information, read Romy Rodriguez Ravines' paper:
The Data Conundrum



The Data Conundrum

Cyber Risk Data. Background and Challenges

Highlights

- Only the second-generation of cyber risk quantification matters: critical Inside-Data is needed to start seeing true, evidence-based, data-driven quantification.
- A few challenges for CRQM:
  - identifying risk factors
  - reliable and relevant data for these risk factors
  - scarce historical data on cyber incidents and financial losses due to cyber risk
  - abundant data in heterogeneous sources and unstructured information on risk factors related to the cyber threat landscape.
- Traditional CRQ industry missed the mark as new OT and IoT sensors and telemetry became readily available and implemented.

Certainly, Cyber Risk Quantification is receiving more and more attention. "***At DeNexus, it is our mission to build the global standard of industrial cyber risk quantification for Industrial OT Asset Owners, shareholders, boards, and insurers."*** ***Romy Rodriguez Ravines*****.**

> *"At DeNexus, it is our mission to build the global standard of industrial cyber risk quantification for Industrial OT Asset Owners, shareholders, boards, and insurers."*
>
> — Romy Rodriguez Ravines, Head of Research & Modelling Strategies at DeNexus

The main hurdles identified in generally accepted literature for modelling, designing, and building systems that quantify cyber risk are as follows:

- the challenges involved in identifying thorough cybersecurity risk factors
- the scarcity of reliable and relevant data for these risk factors
- the lack of systematic procedures for storing relevant data
- the partial view of the problem
- data surety and privacy protection

But, at the same time, new sensors, new telemetry that monitor systems, and new cyber threat intelligence solutions are being introduced and implemented at Industrial OT sites around the world. The existing cyber risk assessment market may have missed the mark by not accessing, leveraging or modeling against the critical Inside-Data that comes out of that telemetry in real-time. Therefore, **there is a gap in the generation of cyber data and relevant and actionable knowledge related to OT/ICS cyber risk**. In short, quantifying industrial cyber risk is hard!

In this context, DeNexus sets out to answer the following questions:

- What data is needed to produce a reliable cyber risk model?
- How can this data be used in the context of cybersecurity/cyber risk?
- When do we have enough empirical data to estimate a reliable model that provides the cyber loss distribution for an organization?

Because ***risk*** is defined as the ***probability*** of a loss event occurring in a given unit of time multiplied by the expected ***magnitude*** of loss resulting from that loss event, the needed information – broadly speaking – is about the organization itself (firmographics), the cyber threats (Outside-Data), the target network, its vulnerabilities and its defenses (Inside-Data) as well as the technical and financial impact caused by each cyber incident over time! **Cyber Risk is dynamic!**

If the purpose of CRQM is both immediate, as well as long-term, management of cyber risk, then modelling to enterprise level risk is required! Gathering information about the business context, underlying industrial processes, the cost and effectiveness of mitigation projects and portfolio exposure is also required. In other words, gathering data for a real evidence based CRQM system is a cumbersome task. **"A knowledge base that brings together the data and intelligence created by this effort is a game changer…and that's the power of the DeNexus Knowledge Center!"** **Juan Carlos Cortinas Abad.**

> *"A knowledge base that brings together the data and intelligence created by this effort is a game changer…and that's the power of the DeNexus Knowledge Center!"*
>
> — Juan Carlos Cortinas Abad, Sr Director of Cybersecurity at DeNexus

The Data Difference. Depth and Breadth

Highlights

- DeNexus Knowledge Center is the unique OT CRQM knowledge base.
- A knowledge base built with structured and unstructured data, from public and private sources, that brings together a 360-degree view of cyber risk.
- With different layers of knowledge: raw data, risk indicators, models insights, aggregated indicators.

DeRISK Platform leverages data from +40 data sources that provide useful information for estimating losses due to cyber risk. This catalog of data sources comprises different leading solutions of telemetry from inside the installations, several of the main solutions that provide data on the cyber threat landscape and attack surface of the organizations, and the most important sources of information about vulnerabilities and disclosed cyber-attacks, among others. *DeNexus Knowledge Center* is the lodge of that information. With in-bound and out-bound dataflows, it is a knowledge base built with structured and non-structured data, from multiple open-source and multiple non-private or proprietary data curation engines.

DeRISK Platform leverages data from +40 data sources that provide useful information for estimating losses due to cyber risk.

DeNexus Knowledge Center holds data, indicators and lessons learned from client's risk assessments, real cyber incidents, and portfolios analysis. The main types of data can be grouped into 4 categories: (1) Inside-Data, (2) Outside-Data, (3) Loss Events, (4) Cyber incidents.

Inside-Data

Sensors in a company's OT network automatically and continuously collect information about the assets, their connections, software, firmware, configuration, and information from the existing control systems. DeRISK has developed integrations with leading OT Asset Management and IDS (Intrusion Detection Systems) tools. The types of data used from inside-out data sources are Asset inventory, Vulnerabilities by assets, Threat detection, Security controls and their Maturity level (inferred indictor), etc. This data is stored in near real-time.

FORESCOUT · NOZOMI NETWORKS · CLAROTY · INDUSTRIAL DEFENDER® · CROWDSTRIKE · tenable · nessus Professional

Inside-Data sources in DeNexus Knowledge Center (January '23)

DeRISK Industrial Benefits

Value Your Cyber Risk
Know your financial risk associated with every cyber risk at all times to make the right capital allocations

Defend Your Operation
Build better cyber defense strategies with detailed posture assessments of every facility under management

Mitigate Risk Exposure
Leverage the DeNexus Knowledge Center for detailed attack-path mapping

ROI-based Cybersecurity
Measure the financial impact of different mitigations to optimize human and financial resources

Leverage Intuitive Interfaces
Reduce cyber risk with visualizations purpose-built for industrial asset owners & insurers

Outside-Data

Data from public and private/proprietary sources, automatically collected and customized for the customer's organization and its supply chain. The outside-in data is updated in daily or weekly basis, depending on the source. The types of data used are as follows:

- **Threat monitoring:** The number of credentials or email accounts found "in the wild".
- **Attack surface:** Information on the client's total external exposure footprint including the number of domains and subdomains, the number of public IP addresses, open ports, vulnerabilities per IP address, threat actors, leaked credentials, etc.
- **Supply chain:** Manufacturers, vendors, OEMs, directly or indirectly associated with the organization.
- **Common Vulnerabilities and Exposures** (CVEs) catalog vulnerabilities found, assessing their criticality in context of each customer and installation from the Common Vulnerability Scoring System (CVSS) score and customer data (Outside-in and Inside-out), and assessing their exploitability from the Exploit Prediction Scoring System (EPSS).
- **Unconventional signals** from multiple external data sources (media mentions in e.g., Twitter, popular news websites, etc.)
- **Threat actor intelligence.** Generation of threat actor intelligence from various external and internal sources to have the detail of potential threat actors updated as needed.
- **Cyber incident data.** Detailed information from disclosed cyber incidents.
- **Social monitoring sources** are used to assess contextual information such as mentions of a company that can increase the attractiveness of a target company or sector

Outside-Data sources in DeNexus Knowledge Center (as for January '23)

Firmographics and Financial Loss Data

Firmographics corresponds to a specific firm or organizations characteristics, including industry, reported revenues and employee count, extracted from public data (or provided by the organization). Public operational and occupational risk datasets on the loss severity associated with different root causes combined with diverse public and proprietary databases on cyber incidents and losses to both quantify financial and nonfinancial impacts, identifying insurable and non-insurable impacts.

Financial loss data is challenging. Organizations are not compelled to explain how the incident occurred or how much money was lost because of it. Most commonly, they might even be required by law or regulations not to make that information public.

This information needs to be addressed by industry vertical.

Financial and Loss Data sources in DeNexus Knowledge Center (as for January '23)

Cyber Incidents Data

Although there are several alternatives for cyber incidents data repositories, this type of information is scarce. While there are many observations in the databases, most variables are sparsely populated. This issue is compounded by the lack of relevant incident data, like security posture at the time of the incident.

DeNexus Knowledge Center contains information on cyber incidents from public databases. This information is obtained in two levels of aggregation:

- **Single incidents data**
  - List of disclosed OT cyber incidents published by the OT community
  - List of disclosed cyber incidents and data breaches published by the most relevant providers of repositories
- **Aggregated incidents data**
  - Aggregated data on cyberattacks published by 3rd-party vendors on a regular basis – annually or semi-annually-. These reports – unstructured data – provide useful information such as the distribution of cyber incidents by region, industry, company's size, etc.

Cyber incidents database sources in DeNexus Knowledge Center (as for January '23)

Cyber incidents metadata sources in DeNexus Knowledge Center (as for January '23)

In short, combining critical data from inside the client's OT network, together with outside threat, loss and vulnerability data opens an entirely new world of cyber risk quantification and management to the Industrial OT /ICS landscape. And that's why we call DeRISK the Second Generation of Industrial Cyber Risk Quantification, Modelling, and Management.

DeRISK - DeNexus Knowledge Center - DeNexus Trusted Ecosystem

The global standard of industrial cyber risk quantification for Industrial OT stakeholders, investors, boards and the risk transfer market

Quantify Cyber Risk. Save Money.

We are DeNexus

DeNexus is the leading provider of cyber risk modeling for ICS/OT organizations and global (re)insurers. Our platform empowers the industrial enterprise and risk underwriters to quantify cyber risk exposure on a continuous, self-adaptive basis using the world's first evidence-based data analytics software and services. The DeRISK Platform from DeNexus is the world's first self-adaptive, cloud-based platform that uses evidence-based data to predict where and how breaches are likely to occur, what their business impact will be and how to mitigate them. DeNexus is headquartered in Sausalito, California with engineering based in Madrid, Spain.

Fortune 500 companies rely on Denexus to understand their bespoke cybersecurity economics and optimize their risk reduction ROI with the SOC 2, type 1 compliant solutions. Leverage DeNexus and our DeRISK Platform to make asset, vulnerable, configuration, operational anomaly, supply chain and cyber intrusion data work for you.

DENEXUS

DeNexus.io
@DeNexusInc1