DENEXUS

Standards in Quantified Industrial Cyber Risk #1

Industrial Cyber Trends and Solutions

As we launch the DeNexus 'Standards in Quantified Industrial Cyber Risk' series, our CEO Jose Seara reflects on 2022 trends, discusses 2023 challenges and offers potential cyber risk solutions to the Industrial OT critical infrastructure market and the Insurers that underwrite their risk.

Increased Threats and Severity

2022 was an unprecedented year for the Industrial cybersecurity space. It kicked off with cybersecurity teams working overtime around the world in January to identify their exposure to Log4j vulnerabilities embedded throughout a large part of their infrastructure. Log4j illustrated how widespread the software supply chain is affected by shared libraries embedded in thousands of software and hardware solutions. It has increased awareness in software bill of materials (SBOM) and third-party supply chain risk.

> *From malware to ransomware and blackouts, 2022 had many challenges for the cyber security landscape.*

In February 2022, Russia invaded Ukraine in a major escalation of the Ukraine War. Russian cyber-attacks against Ukraine have persisted for years, including blackouts in 2015, but intensified just before the 2022 invasion. These attacks have affected Ukrainian critical infrastructure, power outages, and more. Any nation that opposed the Russian government, became a target of ransomware operators.

Within a few months, three European wind energy companies were compromised. Deutsche Windtechnik AG, Nordex SE and Enercon GmbH, impacting remote-control systems for thousands of wind power generators across Europe. Some attacks were claimed by groups supporting the Russian government, and some took place at the same time Russian troops invaded Ukraine.

In April, researchers discovered PIPEDREAM malware built specifically to damage industrial control systems (ICS) with the express purpose of disrupting industrial processes. This malware can communicate natively with control systems with

impacts significantly worse than information loss, but cyber-physical. ICS-specific malware is capable of causing loss of view, loss of control or safety integrity of cyber-physical systems such as pumps, motors, that operate CI like pipelines, generation stations, substations, and more. Dragos said that Pipedream is the seventh known ICS-specific malware, following Stuxnet, Havex, Blackenergy 2, CrashOverride/Industroyer, Trisis/Triton, and Industroyer2. Year over year, there are more ICS-specific attacks, and their sophistication is increasing.

78%

increase in high-severity vulnerability disclosures from 2020 to 2022.

In its December 2022 report on cybersecurity vulnerabilities in ICS/OT, Microsoft reported a 78% increase in high-severity vulnerability disclosures from 2020 to 2022. This means that there are more opportunities than ever for malware to specifically target industrial control systems and have significant impacts.

Regulatory, Compliance and Insurance. Developments and Challenges.

After the Colonial Pipeline ransomware event in 2021 lead to widespread fuel shortages due to pipeline shutdown, the US Transportation Safety Administration (TSA) has continued to enhance its cybersecurity directives for pipelines, it has also expanded them to transportation sectors.

On March 15, the Cybersecurity Incident Reporting for Critical Infrastructures Act of 2022 was signed into law, requiring companies that are attacked to report significant cyber incidents.

Also in March, SEC Proposed Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, aiming to standardize disclosures to investors of material cybersecurity incidents and to improve visibility the cybersecurity risk management and governance policies, making cybersecurity mission-critical for senior executives and boards of directors. SEC's Fact sheet summarizes the new requirements including reporting about material cybersecurity incidents on Form 8-K, periodic disclosures regarding policies, procedures, boards of directors required expertise, etc.

FERC Chairman said in December that he wants to Update Cybersecurity Requirements, including the questioning of high, medium and low categories currently in use to assess compliance with CIP standards, noting that "adversaries can get access to a facility that would have a high impact, if breached through one where such a breach would be considered more low-impact".

At the end of the year, NIS 2 Directive was announced and will improve cybersecurity risk management and will introduce new reporting obligations across sectors such as energy, transport, health, and digital infrastructure. Overall, the scope of NIS2 has widened and now includes more entities that must comply.

> *...underwriters sent a clear message that they are reluctant to accept additional cyber risk without evidence-based data that shows a clearer picture of an insured's cyber exposure.*

In August, the Wall Street Journal reported that Lloyds will Exclude Catastrophic Nation-Backed Cyberattacks from Insurance Coverage. With insurance premiums increasing and coverage decreasing, underwriters sent a clear message that they are reluctant to accept additional cyber risk without evidence-based data that shows a clearer picture of an insured's cyber exposure.

For additional information read our paper on Unlocking Cyber Risk for Insurance Linked Securities.

Industry Observations and Predictions.

The era of voluntary cybersecurity management is over and will be replaced by mandatory cybersecurity compliance and regulations affecting every country and every industry in some way. Failure to comply historically lands the offending organization with negative publicity and a fine, but liability is now going to start including individuals on the Board of Directors. Gartner predicts 40% of Boards will have dedicated cybersecurity committees by 2025.

> *Gartner predicts*
>
> **40%**
>
> *of Boards will have dedicated cybersecurity committees by 2025..*

In the SANS State of ICS/OT Cybersecurity in 2022 report, respondents placed increased visibility into control system cyber assets and configurations' at the top of their list of initiatives. But is that enough?

We think that visibility on the assets is a mandatory first step, but much more needs to be done. Fundamentally, **we believe that industrials continue to struggle to understand the cyber risk coming from their** assets, vulnerabilities and controls. They have not been presented with a way to contextualize that risk with their underlying industrial processes to truly understand their cyber exposure in financial terms, how to manage that risk and eventually how to efficiently and measurably mitigate or transfer it.

It seems that Industrial Asset Owners have been left with more questions than answers. With the increased probability of an attack and regulatory compliance requirements going up, Industrials are forced to ask themselves:

- How do we manage the unknown?
- How do we justify investments in cybersecurity without understanding the true impact of the risk?
- How do we justify and prioritize our cyber investments based on ROI?
- How do we prioritize investments in cyber risk vs our other corporate risks?

Unfortunately, the vast majority of cyber-risk tools that have saturated the market are predominantly based on human input questionnaires, outside-in scanning technology and publicly available breach data, which ultimately delivers, at best, an educated guess.

> *And therein lies the largest gap in cyber risk for Industrial Asset Owners and Insurers...an educated guess, is still a guess*

And therein lies the largest gap in cyber risk for Industrial Asset Owners and Insurers...an educated guess, is still a guess. This approach has proven itself to be inefficient for both the Asset Owner, who's left with the high likelihood of misallocating human and/or capital resources, and for the Insurers, who are already signaling that they are no longer comfortable underwriting against the current industry's 'best-guess' approach to cyber risk.

This is especially true for OT/ICS environments where outside-in only scanning can't provide enough information, data, due to the special characteristics of those environments and how they are protected from the outside world.

Cyber risk is a complex, human made, dynamic risk. **Modeling and assessing evidence-based cyber risk exceeds the capabilities of traditional assessments.** Even the best reports and audits performed by excellent experts in the field become immediately obsolete due to the intrinsic dynamic nature of the risk, impacted by a myriad of ***internal*** and ***external*** drivers. Processing that information requires complex data models and significant computing resources. Plus, extreme care to the security of the data, so the analysis itself does not become another risk factor.

Is there a way to stop guessing and quantify cyber risk?

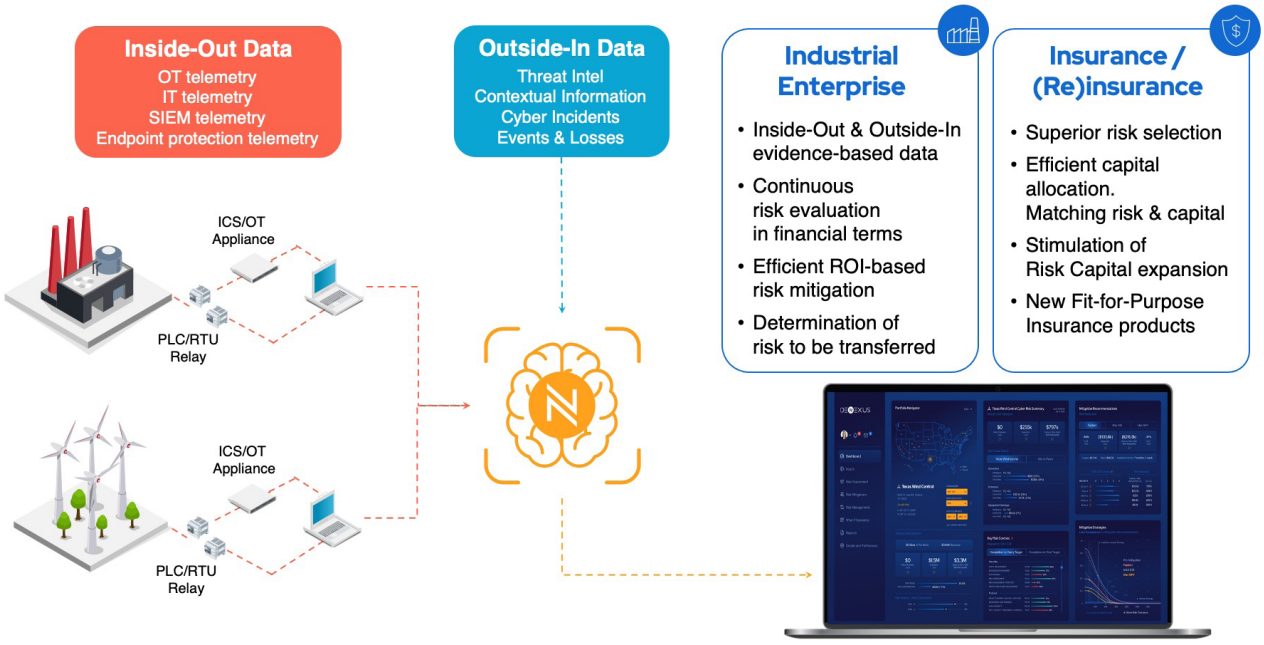
The good news is, there is! While the existing cyber risk assessment tools have been focused on an outside, top-down view of an asset owners' risk, DeNexus has revolutionized the cyber risk modeling, quantification and management industry with its flagship product **DeRISK**!

For the first time, Industrial Asset Owners, (re)Insurers and ILS funds are provided with evidence based, real-time, visibility into their actual asset exposure using data from INSIDE the clients OT network. This Inside Data enables detailed, bottom-up, portfolio-level cyber risk modeling that the entire industry has been missing until now.

Tailored solutions specialized in OT/ICS environments are needed, including the access to highly relevant inside-out data about assets in the ICS/OT environment, vulnerabilities, and controls. Including events and incidents when they occur. Combining that inside data with outside threats, footprints, proprietary attractiveness indicators, etc., opens an entire new world of cyber risk quantification and management capabilities.

For the first time, Industrial Asset Owners, (re)Insurers and ILS funds are provided with evidence based, real-time, visibility into their actual asset exposure using data from INSIDE the clients OT network. This Inside Data enables detailed, bottom-up, portfolio-level cyber risk modeling that the entire industry has been missing until now.

DeRISK represents the Second Generation of Cyber Risk Quantification and Management solutions for ICS/OT environments and industrial companies in the world. This means a fit-for-purpose solutions tailored to each industry and subindustry vertical. It means using ***real-time, inside-sourced*** and ***outside-sourced*** data comprising a large set of multiple public, private and proprietary data sources to build a holistic view of all the factors that affect the cyber risk in an industrial organization, allowing for dynamic responses to fast-changing cyber threats.



DeRISK - Quantify, Manage, Transfer Cyber Risk

DeRISK empowers the Industrial Enterprise and Critical Infrastructure asset owners and operators to evaluate their cyber risk in financial terms, optimize the use or risk management resources providing a ROI-based set of mitigation strategies, and the determination of the quantum of risk to be transferred. It answers the questions that are necessary for efficient management of the cyber risk:

- How much risk do I have
- How do I compare with my industry peers
- Where is the risk coming from?
- How does it evolve over time?
- What can I do to efficiently manage and mitigate the risk?

Providing reports for the different stakeholders, cyber-SMEs, risk managers and executives, breaching the communication gap.

Now that you understand your risk, you can make informed risk management decisions. Now you can budget for risk management investments and explain the return on that. Now you can measure the effectiveness of the investments made and the controls deployed. Now you can efficiently negotiate the transfer of some risk and the premium to pay for that risk transfer.

It also empowers the Insurance industry for a superior selection of the risk, efficient capital allocation, loss reserving and portfolio risk management, the development of new fit-for-purpose insurance products leveraging real-time evidence-based data, and the stimulation of risk capital expansion.

DeNexus is bridging the chasm between risk owners and risk assumers. No more asymmetry in the understanding of the risk.

In future blog posts we will go deeper on how that is achieved. What are the different modules and how they work together and are constantly tested, calibrated and validated to produce trusted, auditable cyber risk numbers, leveraging our industrial cyber risk modeling platform DeRISK, with our proprietary ***DeNexus Knowledge Center***, the brain of our ecosystem, and our ***DeNexus Trusted Ecosystem***, a combination of data integrity, encryption and anonymization tools, security standards and certifications, trusted and certified infrastructure, policies and procedures to enable a strict control over the collection, storage and dissemination of highly sensitive cyber data.

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

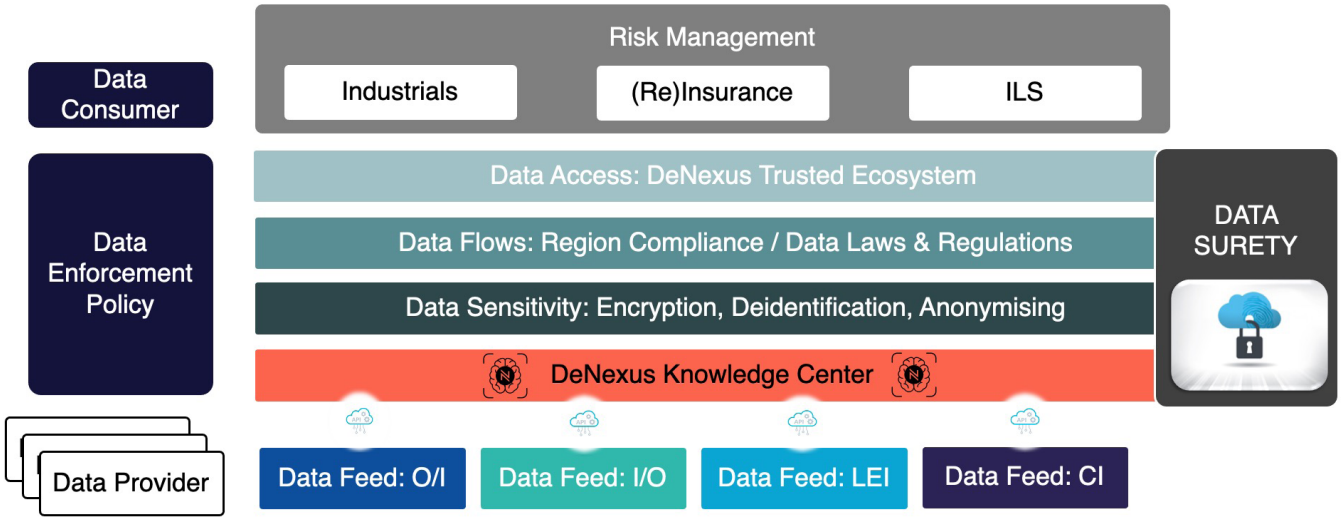
Mitigate Risk Exposure
Leverage the DeNexus Knowledge Center for detailed attack-path mapping

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

DeRISK - Key Components

And on how the highly sensitive data is retrieved, storage and shared among the different users complying with the most stringent business and compliance standards.



DeNexus Trusted Ecosystem: Data Insights Platform

Combination of data integrity, encryption and anonymization tools, security standards and certifications, trusted and certified infrastructure, policies and procedures - Strict Control over the Dissemination of Data

DeRISK - DeNexus Knowledge Center - DeNexus Trusted Ecosystem

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